VILNIAUS UNIVERSITETAS
INFORMATIKOS INSTITUTAS
PROGRAMŲ SISTEMŲ KATEDRA

# Išskirstyto transakcijų žurnalo technologija tiekimo grandinės procesuose

## Distributed Ledger Technology in Supply Chain Processes

Bakalauro baigiamasis darbas

| | | |
|---|---|---|
| Atliko: | Gediminas Krasauskas | (parašas) |
| Darbo vadovas: | dr. Evaldas Drąsutis | (parašas) |
| Darbo recenzentas: | partn. doc. Andrius Adamonis | (parašas) |

Vilnius – 2019

Nuoširdžiai dėkoju savo darbo vadovui Dr. Evaldui Drąsučiui už darbo metu teiktą konstruktyvią kritiką ir pagalbą.

# Santrauka

Šiame darbe nagrinėjamos IOTA platformos panaudojimo galimybės konkrečiuose tiekimo grandinės procesuose. Darbe analizuojama tiekimo grandinių dalykinė sritis, jos sąvoka, struktūra ir problemos. Aprašyta išskirstyto transakcijų žurnalo technologija bei jai keliami reikalavimai tiekimo grandinių kontekste. Išanalizuotos technologijos atmainos, paremtos blokų grandinės ir orientuoto grafo be ciklų principais, pristatytos jų savybės, privalumai ir trūkumai. Sukonstruotas pavyzdinis tiekimo grandinės modelis ir diskretūs IOTA platformos taikymo atvejų pavyzdžiai konkrečiuose etapuose, skirti pagrįsti platformos panaudojamumą tiekimo grandinėse. Pateiktos taikymo alternatyvos. Darbe pasiūlytos potencialios sistemos svarbiausios užduotys ir veiklos, reikalingos praktinio taikymo įgyvendinimui.

**Raktiniai žodžiai: Tiekimo grandinė, išskirstytas transakcijų žurnalas, blokų grandinė, orientuotas grafas be ciklų, IOTA.**

# Summary

This paper explores the possibilities of using the IOTA platform in specific supply chain processes. The thesis analyzes the subject area of supply chains, its concept, structure and problems. The distributed ledger technology and its requirements in the context of supply chains are described. The types of technology based on the principles of blockchain and directed acyclic graphs were analyzed, their properties, advantages, and disadvantages were presented. An exemplary supply chain model and discrete examples of the application of the IOTA platform at specific stages were designed to support the usability of the platform in supply chains. Application alternatives provided. The thesis suggests the most important tasks and activities of the potential system to implement the practical application.



**Keywords: Supply chain, distributed ledger, blockchain, directed acyclic graph, IOTA.**

**TURINYS**

# Įvadas

Modernią visuomenę sunku įsivaizduoti be nuolatinio prekių, paslaugų ir informacijos judėjimo. Prekės transportuojamos iš vienos vietos į kitą, internetu perduodami milžiniški srautai informacijos, atliekamos transakcijos tarp skirtingų verslo šalių. Tačiau natūraliai pamatyti šiuos procesus vis dėlto nėra toks lengvas uždavinys. Visi šie procesai yra paslėpti po sudėtingomis verslo taisyklėmis, modeliais ir technologijomis.

Apskritai šie sudėtingi procesai kuria milžinišką pridėtinę vertę, o kartu gerina ir bendrą pasaulinį ekonomikos lygį. Pavyzdžiui, logistika sudaro 7,5% JAV BVP[1], o duomenų srautai 2014 metais prie pasaulinio BVP lygio prisidėjo $2.8 trln. JAV dolerių [MLB+16]. Todėl, siekiant verslo progreso ir konkurencinio pranašumo, šiuos procesus stengiamasi kuo labiau optimizuoti bei automatizuoti. Atrodo, kad tai pasiteisino. Per pastaruosius dešimtmečius žmonija tapo gerokai pažangesnė: visuomenės kompiuterinis raštingumas išaugo [DD15], o kartu skaitmenizavosi ir verslas – pradėtos naudoti sudėtingos IT sistemos ir sprendimai.

Pasaulyje esant per 7,5 mlrd. žmonių ir šiam skaičiui vis dar augant[2,3] bei gerėjant ekonominėms sąlygoms, kartu nenumaldomai auga ir vartojimas[4], o klientai kelia vis aukštesnius reikalavimus [Nil06]. Taigi, norėdamos išlikti konkurencingomis, įmonės varžosi tarpusavyje, naudoja įvairias laiko optimizavimo strategijas, užtikrinančias paslaugų greitį [ZM04], investuoja į vis pažangesnes informacines technologijas. Visa tai tam, kad produktas iš gamintojo į pirkėjo rankas patektų kuo kokybiškiau ir optimaliau.

Šis produkto gyvavimo ciklas, nuo pradinio tiekėjo iki galutinio kliento rankų, yra vadinamas tiekimo grandine. Tačiau šis apibrėžimas nenusako, kokios apimties ir sudėtingumo logistika vyrauja tiekimo grandinėse. Vien 2017 metais buvo pasiekta apie 750 mln. TEU standarto jūrinių konteinerių krova[3], o tais pačiais metais Klaipėdos uosto metinė krova viršijo 43 mln. tonų[5]. Ir tai tik jūrų krovinių dalis. Remiantis Transparency Market Research duomenimis, iki 2023 metų pajamos visoje logistikos rinkoje turėtų išaugti iki $15,5 trln. JAV dolerių, o krova iki 92 mlrd. tonų[6].

[1]Informacija paimta iš: https://www.atkearney.com/transportation-travel/article?/a/2017-state-of-logistics-report-article [žiūrėta 2019-05-14].

[2]Informacija paimta iš: http://www.worldometers.info/world-population [žiūrėta 2019-05-14].

[3]Informacija paimta iš: https://www.google.com/publicdata/directory [žiūrėta 2019-05-14].

[4]2012-2017 metais visuotinis BVP padidėjo nuo $70 trln. iki $80 trln. JAV dolerių. Informacija paimta iš: https://www.google.com/publicdata/directory [žiūrėta 2019-05-14].

[5]Informacija paimta iš: https://sumin.lrv.lt/lt/naujienos/klaipedos-uostas-lyderis-regione [žiūrėta 2019-05-14].

[6]Informacija paimta iš: https://www.prnewswire.com/news-releases/global-logistics-market-to-reach-us155-trillion-by-2023-research-report-published-by-transparency-market-research-597595561.html [žiūrėta 2019-05-14].

Šie duomenys nepaprastai svarbūs, nes leidžia suprasti, kokią naudą visai žmonijai ir galimybes rinkai gali atverti IT sprendimų sėkmingas taikymas tiekimo grandinėse. Tiesa, įmonės, užsiimančios logistika ir tiekimo grandinių valdymu, tą iš dalies jau atlieka. Tai programinė įranga ir technologijos, tokios kaip CRM [BC15], ERP [NOB18] ir daugelis kitų. Tačiau visi jie turi savų trūkumų ir nėra tinkami kiekvienai tiekimo grandinei [GSS18].

Yra teigiama, kad šiandieninėms problemoms spręsti tiekimo grandinėse į pagalbą gali ateiti daiktų internetas [DHP17] ir iki tol dar plačiai netaikyta išskirstyto transakcijų žurnalo technologija [AM16]. Daiktų internetas padėtų sekti produktų būseną gyvavimo ciklo metu. To pavyzdys – šiuo metu naudojami RFID prietaisai, galintys perduoti informaciją realiu laiku [MR17]. Tuo tarpu išskirstyto transakcijų žurnalo technologijos plačiau žinomos dėl vienos iš atšakų – blokų grandinės. Tačiau vis didesnes perspektyvas rodo IOTA platforma [Pop16], paremta kita atšaka – orientuotais grafais be ciklų. Jos kūrėjai teigia, jog ši yra pritaikyta būtent daiktų internetui ir tiekimo grandinėms.

Tyrimo objektas – išskirstyto transakcijų žurnalo technologijos vienos iš atmainų panaudojimas tiekimo grandinėje. Šiuo metu tai yra technologija, neturinti daug įgyvendintų ir pripažintų pavyzdžių tiekimo grandinių procesuose. Taip pat nėra aišku, kuri technologijos atmaina yra parankesnė ir kokiais konkrečiais būdais įgalinti technologiją.

**Darbo tikslas** – pateikti išskirstyto transakcijų žurnalo technologijos sprendimus tiekimo grandinės procesuose.

**Darbo uždaviniai**:

1. Apžvelgti tiekimo grandinės dalykinę sritį: jos svarbiausias sąvokas, struktūrą ir problemas;
2. Išanalizuoti išskirstyto transakcijų žurnalo technologiją ir jos atmainas: blokų grandinę ir orientuotą grafą be ciklų, juos palyginti;
3. Sukonstruoti pavyzdinį tiekimo grandinės modelį ir, taikant vieną iš išskirstyto transakcijų žurnalo technologijos atmainų, jį atnaujinti;
4. Pateikti potencialios sistemos esmines užduotis ir veiklas.

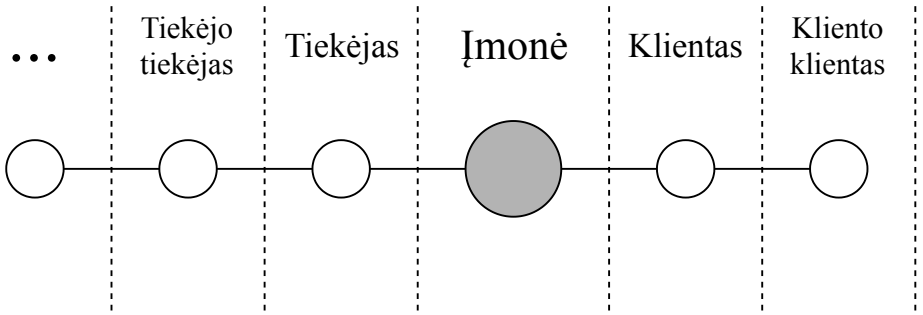
# 1. Tiekimo grandinė

Tam, kad būtų galima nagrinėti technologijų taikymą tiekimo grandinėse, reikia suprasti dalykinę sritį, t.y. kokios yra svarbiausios sąvokos, struktūra, vyraujančios problemos ir keliami reikalavimai. Dėl šios priežasties tolimesniuose poskyriuose bus apžvelgiami išvardyti tiekimo grandinės aspektai.

## 1.1. Sąvoka

Tiksliai ir vienareikšmiškai apibrėžti tiekimo grandinę (angl. *Supply chain*) yra ganėtinai sunkus uždavinys. Apskritai, tai yra pakankamai abstrakti sąvoka, kuri kuri laikui bėgant evoliucionavo ir galinti kisti nuo konteksto, kuriame yra naudojama. Pavyzdžiui, grupė akademikų tiekimo grandinę apibrėžė kaip tris arba daugiau šalių, tiesiogiai susijusių su produktų, paslaugų, finansų ir informacijos judėjimo srautais nuo šaltinio iki kliento [MDK+01]. Tuo tarpu Martin Cristopher tiekimo grandinę įvardijo kaip dalyvaujančių organizacijų tinklą, kuris skirtingais procesais ir veiklomis kuria vertę produktų ir paslaugų pavidalu vartotojui [Chr16].

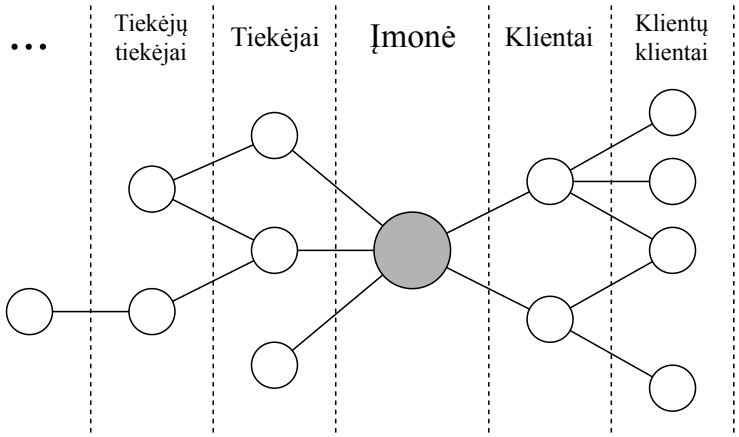
Taip pat Martin Cristopher savo knygoje diskutuoja, kad tiekimo grandinės sąvokoje žodis *tiekimo* turėtų būti pakeistas žodžiu *paklausos* (angl. *Demand*), o žodis *grandinė* – žodžiu *tinklas* (angl. *Network*). Paklausos sąvoka argumentuojama tuo, kad tiekimo grandinė priklauso ne nuo tiekėjų, o nuo rinkos situacijos, t.y paklausos, o tinklo sąvoka labiau atitiktų struktūrą, kadangi paprastai tiekimo grandinėje dalyvauja daugiau nei vienas tiekėjas ir klientas [Chr16]. Tokiu būdu tiekimo grandinės modelis (žr. 1 pav.) taptų panašesnis į paklausos tinklo modelį (žr. 2 pav.).




1 pav. Tiekimo grandinės modelis [Chr16]

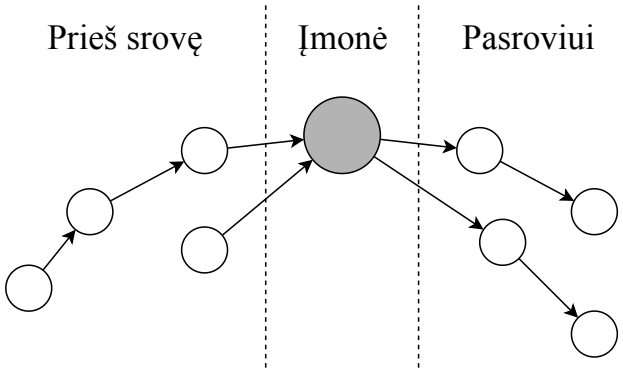
Nors tinklo modelis yra arčiau realybės, tačiau dėl paprastumo ir platesnio sąvokos žinomumo šiame darbe tiekimo grandinės sąvoka bus naudojama turint omenyje tinklo struktūrą. Taigi, pasinaudojus abiem moksliniais šaltiniais, galima suformuluoti išvestinį tiekimo grandinės apibrėžimą – tai organizacijų, procesų, finansų, informacijos ir kitų esybių visuma, dalyvaujanti produkto

gyvavimo cikle nuo pradinio tiekėjo iki galutinio kliento.




2 pav. Paklausos tinklo modelis [Chr16]

Daugelyje mokslinių straipsnių galima aptikti sąvokas *prieš srovę* (angl. *Upstream*) ir *pasroviui* (angl. *Downstream*) [CD05; FW01; VK06]. Tiekimo grandinės kontekste šie žodžiai reiškia įmonės sąryšį su tiekėjais ir klientais. Pavyzdžiui, viską, kas ateina į įmonę iš tiekėjų, paprastai ateina prieš srovę. Tuo tarpu tai, kas išeina iš įmonės pas klientus, atvirkščiai, pasroviui [Chr16] (žr. 3 pav.). Prieš srovę ir pasroviui gali judėti ne tik prekės, bet ir pinigai, informacija bei kitos esybės.




3 pav. Įmonės sąryšiai su tiekėjais ir klientais [Chr16]

## 1.2. Struktūra

Nagrinėjant tiekimo grandinės sąvoką 1.1 poskyryje buvo išsiaiškinta, kad yra tiekėjų, klientų ir įmonės rolės. Tačiau tai yra pernelyg abstraktus modelis, kuris nesuteikia gilesnių žinių apie tiekimo grandinės veikimą. Šiame darbe svarbu suprasti kas yra tie tiekėjai ir klientai bei kaip šalys bendrauja tarpusavyje, t.y. kokios veiklos ir procesai vyksta tiekimo grandinėje.

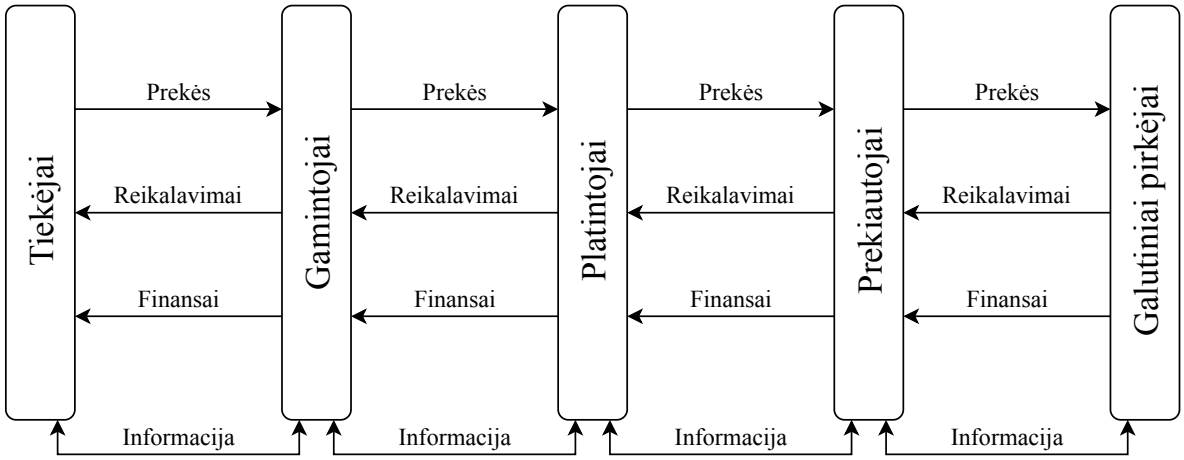
Tačiau visa tai labai priklauso ir nuo industrijų, kuriose šios tiekimo grandinės funkcionuoja.

Pavyzdžiui, procesai ir praktikos, naudojamos maisto pramonėje nebūtinai gali tikti automobilių gamybos industrijoje. Tą patvirtina vien saugumo klausimų skirtumai tarp šių pramonių [MGM+11].

Nagrinėti tikslią realybėje egzistuojančias tiekimo grandinės struktūras yra sunku ir dėl to, kad įmonės neviešina savo tiekimo grandinės tikslaus gyvavimo ciklo dėl konfidencialumo ir konkurencinių priežasčių. Tačiau įvairiuose šaltiniuose galima aptikti nemažai pavyzdinių realybę bandančių atkartoti modelių nuo pat žaliavų surinkimo iki pagaminto produkto pristatymo galutiniam pirkėjui [Chr16; Har16; LCP17; WL09]. Pasinaudojus jais, buvo sumodeliuotas pavyzdinis tiekimo grandinės modelis, aprašytas 3.1 poskyryje.

Paprastai fizinių produktų tiekimo grandinėje dalyvauja: tiekėjai (angl. *Suppliers*), gamintojai[7] (angl. *Manufacturers*), platintojai (angl. *Distributors*), prekiautojai (angl. *Retailers*) ir galutiniai pirkėjai (angl. *End Customers*) [KJ03]. Taip pat bet kurioje grandies etape gali dalyvauti išorinės šalys, tokios kaip audito įmonių arba muitų inspektoriai [WL09].

Įvairiuose straipsniuose yra diskutuojama, kad fiziniai produktai keliauja į įmones prieš srovę ir išeina iš įmonės pasroviui, o informacija apie turimus produktus[8] atvirkščiai – į įmonę patenka pasroviui, o išeina prieš srovę [CD05; PO12]. Tačiau ne mažiau svarbu, kaip juda finansai, keliami reikalavimai ir informacija apie produktus.




4 pav. Tiekimo grandinės esybių srautų judėjimas

Užsakymus paprastai inicijuoja pasroviui esantys tiekimo grandinės nariai [CD05]. Tai reiškia, kad finansus ir keliamus reikalavimus teikia taip pat pasroviui esantys grandinės nariai. Tuo tarpu detali informacija apie produktus ir jų kokybę į įmones patenka prieš srovę. Tai gali būti socialiai atsakinga informacija[9], susijusi su aplinkosauga, darbuotojų darbo sąlygomis, cheminių

[7] Į šią kategoriją įtraukiami pramonininkai, apdirbėjai.

[8] Ši informacija naudinga tiekėjams sužinoti apie paklausą, t.y. koks užsakovo poreikis [CD05].

[9] Šios informacijos poreikis kyla iš keliamų reikalavimų.

produktų naudojimu ar inspektorių vertinimais [MAS15; VK06]. Taip pat duomenys apie prekių laikymo sąlygas, lokaciją, kokybę ir t.t. 4 paveikslėlis vaizduoja įvairių esybių judėjimą tarp šiame poskyryje išvardytų tiekimo grandinės narių.

## 1.3. Problemos

Natūralu, kad įmonėms, dalyvaujančioms tiekimo grandinėse, tenka užduotis suvaldyti visus esybių srautus. Tam į pagalbą ateina IT sprendimai, kurių vienas – verslo valdymo sistemos (angl. *Enterprise Resource Planning*), toliau – ERP. Tai yra programinė įranga, kuri apjungia visus įmonės duomenis ir procesus, arba paprasčiau – duomenų bazė, kurioje gali būti laikomi įvairūs duomenys [ÖÇ16].

ERP turi savo privalumų. Sistema leidžia matyti bendrą verslo vaizdą, suteikdama duomenų bazę su visomis transakcijomis, kurias galima įrašyti, stebėti ir apdoroti [NOB18]. Taip yra pasiekiamas pagrindinis tikslas – centralizuotas įmonės valdymas [ÖÇ16]. Tačiau dalis įmonių vis dėlto nesirenka ERP dėl aukštos sistemų kainos, ilgo adaptacijos laikotarpio ir įmonės vidinių technologinės infrastruktūros nepajėgumų [ÖÇ16]. Dar viena svari priežastis – tradicinės ERP sistemos neleidžia stebėti individualių produktų [GSS18].

Ir tai tik programinės įrangos pavyzdys. Tiekimo grandinės apimtis yra plati, todėl visose jos grandyse kyla skirtingos problemos. Pavyzdžiai: gendantys produktai dėl prastovų [BCG+10], pasimetantys dokumentai ir kroviniai [HM07], socialinės ir gamtosaugos problemos [MAS15; VK06], produktų padirbinėjimai [HM07] ir dar daug kitų. Šios problemos indikuoja, kad yra poreikis IT technologijoms, kurios užtikrintų jų prevenciją. Potenciali dalį problemų išspręsti siekianti technologija bus apžvelgiama kitame skyriuje.

# 2. Išskirstyto transakcijų žurnalo technologija

Kadangi problemos tiekimo grandinėse yra nepašalintos, tai reiškia, kad tradiciniai sprendimai ir technologijos, naudojamos jose, vis dėlto neveikia taip gerai, kaip norėtųsi. Tačiau bet kuriuo atveju, norint vykdyti įmonės apskaitą ir talpinti įrašus ar transakcijas, teks naudotis transakcijų žurnalo (angl. *Ledger*) paslaugomis. O tas, kas teikia transakcijų žurnalo paslaugas, turės įgyvendinti duomenų bazę, kad būtų galima valdyti duomenis.

Tačiau pagrindinė problema kyla dėl to, kad dalyvaujant pirkėjams ir pardavėjams, bei fiksuojant atliekamas transakcijas, yra reikalingas tarpininkas [GXC+18], kuriuo pasitikėtų visos sistema besinaudojančios šalys. Transakcijų žurnalo centralizuotas valdytojas savaime tampa vienvaldžiu tarpininku ir vieninteliu tiesos šaltiniu (angl. *Single source of truth*), o tai suteikia perteklinę įtaką ir galią įrašų manipuliavimui bei kitas potencialias grėsmes [Jia17; SP18].

Vienas populiariausių transakcijų žurnalo tarpininko pavyzdžių – bankas. Bankai yra tarpininkai tarp skirtingų šalių, kurios nori atlikti transakcijas tarpusavyje bei laikyti įrašus apie turimą turtą. Bankai sėkmingai gyvuoja dėl to, kad naudotojai, neturėdami kitos išeities ar alternatyvų, pasitiki jais. Tačiau šis pasitikėjimas turi ir savų rizikų. Bankinė institucija potencialiai gali susikompromituoti ir pradėti keisti, ištrinti įrašus savo naudai, taikyti mokesčius už tarpininkavimą ir pasisavinti turtą [SP18]. Tai yra priežastys, dėl kurių transakcijų žurnalo naudotojai negali iki galo pasikliauti tokiais tarpininkais.

Neseniai vis daugiau susidomėjimo susilaukė išskirstyto transakcijų žurnalo technologija (angl. *Distributed Ledger Technology*), toliau – DLT. Pagrindinė priežastis, kodėl ji atkreipė rinkos, o ypač tiekimo grandinėse ir logistikoje esančių dalyvių dėmesį, yra jos technologinė prasmė. Vienai šaliai priklausantis centralizuotas transakcijų žurnalas pakeičiamas į išskirstytą transakcijų žurnalą, kuris nepriklauso jokiam savininkui, tačiau visi tinklo nariai turi jo kopijas [SP18]. Tai reiškia pagrindinės problemos sprendimą – pašalintą trečiųjų šalių poreikį [SP18]. DLT naudojančiai sistemai nebereikia administravimo, o tuo pačiu ir tarpininko mokesčio. Galiausiai užtikrinamas skaidrumas, pašalinant grėsmę, kad tarpininkas piktavališkai išnaudos turimą galią.

## 2.1. Išskirstyto transakcijų žurnalo savybės

Nors pagrindinis DLT išskirtinumas yra tarpininko pašalinimas, jos unikalumas ir ypatybės tuo neapsiriboja. Šią technologiją būtų logiška tirti iš reikalavimų perspektyvos, kurie kyla iš tikimo grandinėse dalyvaujančių suinteresuotų šalių poreikių. Pagrindiniai poreikiai ir DLT savybės nagrinėjamos tolimesniuose poskyriuose.

### 2.1.1. Greitis

Šio darbo įžangoje jau buvo pabrėžta, kokio dydžio ir masto informacijos srautai bei transakcijų kiekiai vyrauja tiekimo grandinėse. Naudojamas transakcijų žurnalas turėtų būti labai greitas, t.y. gebėti apdoroti šimtus tūkstančių įrašų per labai trumpą laiko tarpą, tiek juos rašant, tiek nuskaitant. Šis rodiklis gali būti matuojamas transakcijomis per sekundę (angl. *Transactions per second*), toliau – TPS, nusakančiu kaip greitai įrašas atsiduria transakcijų žurnale. Natūralu, kad kuo ilgesnis laukimo laikas, tuo daugiau nuostolių gali patirti transakcijų žurnalo naudotojai. Ateityje šie apkrovos rodikliai turėtų nenumaldomai augti dėl vis labiau taikomo daiktų interneto [KGA+18].

Vienas iš įrašų kūrimo pavyzdžių – radijo dažnio identifikavimo (angl. *Radio Frequency Identification*) technologijos, toliau – RFID. Jeigu kiekviename konteineryje, maisto plantacijose, fabrikuose ir t.t. būtų naudojamas vienas ar keli RFID davikliai, kurie paneštų savo būseną numatytu laiko periodu, tai lemtų milijardinius aktyvių tinkle esančių dalyvių kiekius per parą pasauliniu mastu.

Be to, visi šie duomenys turėtų būti saugomi ilgą laiką. Įmonėms gali prireikti prieš kelis metus atliktų transakcijų, vykdytų operacijų arba individualių RFID daviklių istorinių duomenų. Svarbus ir duomenų atsekamumas, kad būtų galima stebėti krovinių kelionę ir būseną, net jei šie duomenys buvo kaupiami tam tikrose vietose neturint interneto ryšio. Greitas ir stabilus visų šių duomenų valdymas tampa sudėtingu IT infrastruktūriniu uždaviniu.

Nors duomenų apdorojimo greitis yra ko gero svarbiausias kriterijus, į kurį turi atsižvelgti technologijos, DLT iš savęs nepateikia sprendimo greičio klausimui spręsti. Tai – konkrečios DLT architektūros klausimas, nuo kurios ir priklauso, kokie sprendimai bus įgyvendinami, norint išpildyti greičio reikalavimus.

Tradicinės transakcijų žurnalų sistemos iš esmės yra išsprendusios greičio klausimus ir gali apdoroti tūkstančius transakcijų per sekundę[10] ar net milijonus transakcijų per sekundę[11]. Tačiau naudojant DLT, dėl savo subtilybių ir specifikos, greičio problemos atsiranda kitu pavidalu. Kiekvieno įrašo padarymas yra konsensuso algoritmo (angl. *Consensus Algorithm*) dalis. Konsensuso algoritmas – tai protokolas, kuris pasirūpina, kad visi tinklo nariai sinchronizuotųsi tarpusavyje ir prieitų bendrą sutarimą įvertinant, kurios transakcijos yra tinkamos, kad jas būtų galima pridėti į transakcijų žurnalą [CV17].

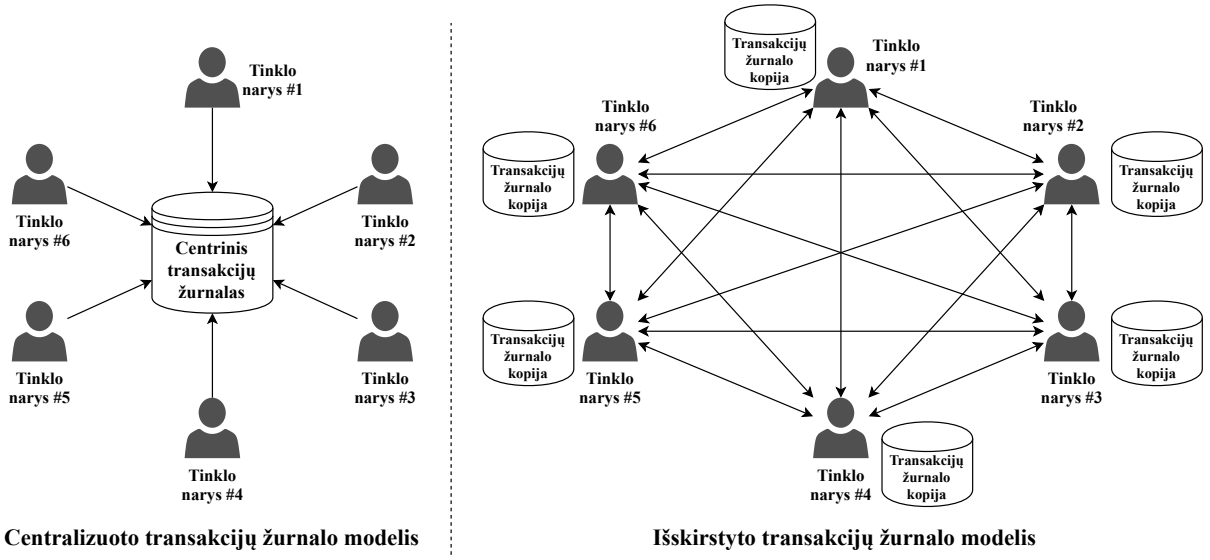
[10] Mokėjimų platformos, tokios kaip PayPal, vykdo apie 136 TPS, o Visa nuo 2 tūkst. TPS iki 56 tūkst. TPS [HP16].

[11] Šiuos rodiklius demonstruoja duomenų bazių valdymo sistemos, tokios kaip Oracle: https://blogs.oracle.com/timesten/scaling-sql-to-millions-of-transactions-per-second-with-a-single-database [žiūrėta 2019-05-14].

### 2.1.2. Duomenų nekintamumas

Tiekimo grandinėse ypatingai svarbu, kad įrašai nebūtų padirbinėjami arba sunaikinami be žinios ar nepageidaujamo įsikišimo. Šiuo metu vyraujant centralizuotoms duomenų bazėms, administratoriai gali manipuliuoti duomenimis, o fizinės duomenų saugyklos, įvykus nenumatytiems incidentams, gali būti pažeistos nepataisomai.

DLT siūlo decentralizuoto transakcijų žurnalo architektūrą (žr. 5 pav.), kurio veikimui nereikia jokios centralizuotos duomenų saugyklos ar administravimo [LYH+18]. Transakcijų žurnalas tampa paskirstytas visame tinkle ir, naudojant konsensuso algoritmą, visi autorizuoti pakeitimai bet kurio vartotojo transakcijų žurnalo kopijoje atsispindi visų tinkle esančių vartotojų kopijose [PMM+18]. Taip yra todėl, kad tinklo nariai, norėdami skaityti arba rašyti informaciją, kreipiasi ne į centrinę duomenų saugyklą, o į tinklą, t.y. tinkle dalyvaujančius narius ir jų duomenis.




5 pav. Transakcijų žurnalo centralizuoto ir išskirstyto tipų modeliai

Iš to kyla viena svarbiausių DLT savybių: tai, kas įrašyta į išskirstytą transakcijų žurnalą, negali būti pakeista arba ištrinta – šitaip yra pasiekiamas duomenų nekintamumas (angl. *Data Immutability*) [XCS+17]. Tokiu atveju visi duomenys tampa apsaugoti nuo potencialaus duomenų padirbinėjimo. O tai leidžia matyti visą unikalią istorinę informaciją. Pavyzdžiui, transportuojant prekes iš taško A į tašką B ir fiksuojant krovinio vietą laike, galime matyti visą jo kelionės istorinę informaciją ir pasitikėti išskirstytu transakcijų žurnalu, jog tie duomenys yra autentiški.

Tą užtikrina jau minėtas konsensuso algoritmas, apsaugantis duomenis nuo piktavalių naudotojų. Tačiau ši savybė tam tikrais atvejais gali būti tuo pačiu ir trūkumas. Pavyzdžiui, kai naudojame informaciją, galinčią dažnai kisti. Pasikeitus kliento mobilaus telefono numeriui, atnaujinti esamo duomenų įrašo negalėtume ir tektų kurti naują įrašą apie atsinaujinusius kliento duomenis.

### 2.1.3. Duomenų saugumas

Svarbu, kad privatūs ir jautrūs duomenys, kuriais disponuoja įmonės, būtų apsaugoti, o prieigą prie jų turėtų tik tie, kam duomenys priklauso arba turi leidimą juos valdyti. Tai tapo dar svarbesniu veiksniu 2018 metais įsigaliojus GDPR reglamentui [Fer18]. Jeigu įmonės paviešintų jautrią informaciją, ji patirtų milžiniškus piniginius nuostolius dėl baudų, o nutekinta įmonei svarbia informacija pasinaudotų jos konkurentai.

Didelė dalis populiariausių DLT yra viešos, nereikalaujančios prieigos teisių (angl. *Permissionless Ledger*), t.y. visi vartotojai turi prieigą prie transakcijų žurnalo [ØUJ17]. Šitaip viešai matoma kas ir kokią informaciją įrašo į paskirstytą žurnalą, o tuo pačiu bet kas gali kurti naujus įrašus. Tačiau galimos ir papildomos DLT konfigūracijos. Pavyzdžiui, galima sukurti tokį privatų išskirstytą transakcijų žurnalą (angl. *Permissioned Ledger*), kuriame duomenis skaityti bei rašyti galėtų tik prieigos teisę turinčios šalys [Bac16]. Tai yra naudinga, jeigu dvi ar daugiau įmonių yra verslo partnerės ir nori dalintis bendra informacija ar atlikti transakcijas tarpusavyje, tačiau jos nenorėtų, kad bet kas kitas už šio rato ribų apie tai žinotų.

Vis dėlto, duomenis apsaugoti galima ir kitais būdais. Pavyzdžiui, naudojant kriptografijos metodus, tokius kaip privatų ir viešą raktą [ZN+15], galime užšifruoti duomenis ir į išskirstytą transakcijų žurnalą įrašyti tik tam tikrą maišos reikšmę (angl. *Hash value*). Tiesa, visi tinklo nariai matys kas šiuos duomenis patalpino, tačiau niekas negalės žinoti duomenų turinio, išskyrus šalis, turinčias privatų raktą. Tai leidžia talpinti jautrią informaciją į viešą DLT ir jaustis saugiai, nes peržiūrėti jos originalų formatą be leidimo, t.y. privataus rakto, negali niekas.

## 2.2. Išskirstyto transakcijų žurnalo atmainos

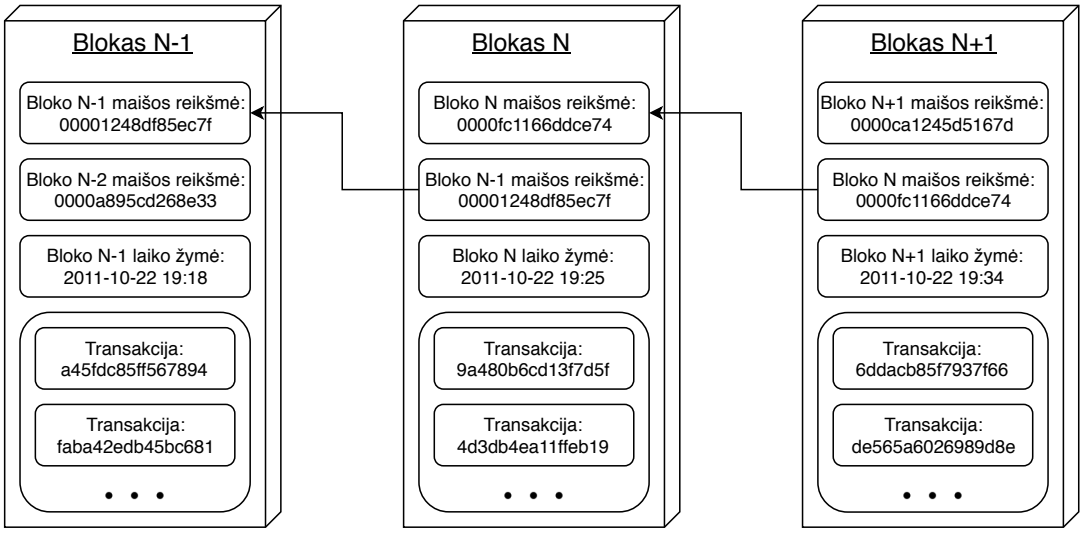
Yra du pagrindiniai DLT tipai. Tai blokų grandinės (angl. *Blockchain*) ir orientuoto grafo be ciklų (angl. *Directed Acyclic Graph*), toliau – DAG struktūrą turintys DLT, kurie bus analizuojami tolimesniuose poskyriuose.

### 2.2.1. Blokų grandinė

Šiuo metu yra daug blokų grandinių projektų, tačiau populiariausiomis ir stabiliausiomis išlieka dvi – Bitcoin ir Ethereum[12]. Šios blokų grandinės veikia tokiu principu: blokų duomenų struktūros, kuriose saugoma informacija, t.y. transakcijos bei kitos blokų grandinės veikimui reikalingos reikšmės, yra sujungtos tarpusavyje nuosekliai į vieną ilgą ir nenutrūkstamą seką (žr. 6

[12]Duomenys paimti iš: https://coinmarketcap.com [žiūrėta 2019-05-14].

pav.)[13]. Vienintelis būdas sukurti naujus įrašus – surinkti juos į naują bloką ir prijungti jį prie paskutinio grandinėje esančio bloko.




6 pav. Blokų grandinės architektūrinis modelis

#### 2.2.1.1. Blokų grandinės duomenų nekintamumas

Jeigu bandytume pridėti bloką grandinės viduryje, ši išsišakotų į 2 atskiras šakas. Čia svarbią reikšmę turi konsensuso algoritmas. Konsensuso algoritmas turi apsaugoti blokų grandinę nuo grandinės išsišakojimų, blokų ištrynimo, keitimo, dvigubo išleidimo problemos (angl. *Double-spending problem*) bei kitokių taisyklių pažeidimų ar spragų, kuriomis norėtų pasinaudoti kenkėjai tinkle [Bal17]. Kitaip – garantuoti duomenų nekintamumą ir vienareikšmiškumą.

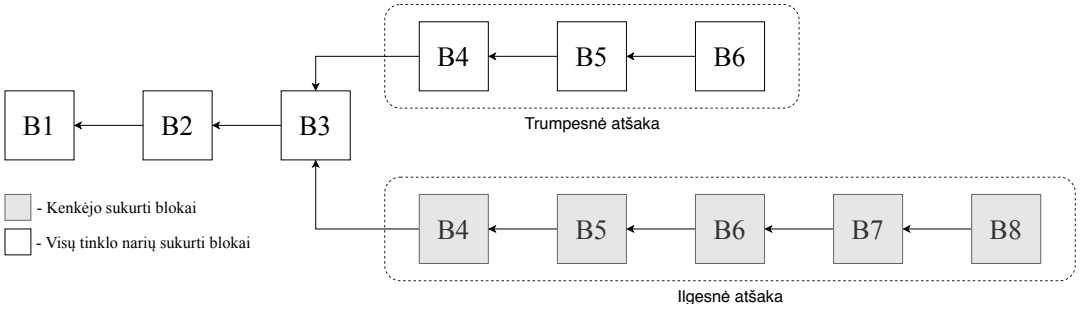
Vienas iš tokių konsensuso algoritmo atmainų, kurį naudoja Bitcoin ir Ethereum, yra atlikto darbo (angl. *Proof of Work*) konsensuso algoritmas, toliau – PoW [GKW+16]. Kaskart norint pridėti bloką, reikia atlikti darbą, kuris reikalauja kompiuterinių skaičiavimų galios, laiko ir energijos išteklių. Blokų grandinėje kuriant naujus blokus tam tikrais atvejais atsiranda išsišakojimų. Tai įvyksta tada, jeigu du ar daugiau blokų iškasami beveik tuo pačiu metu [ZXD+17]. Atsiradus tokiems išsišakojimams, tinklas pasirenka ilgiausią atšaką, t.y. tokią, kuri turi daugiausiai blokų [ZXD+17].

Tačiau išsišakojimus galima kurti ir savanaudiškais tikslais. Tinklo kenkėjas, norintis pakeisti transakciją viename iš blokų, sukurs grandinės išsišakojimą, turintį savyje pakeistos transakcijos versiją. Tačiau tam, kad tinklas pripažintų pakeistą transakciją grandinėje, t.y. naują grandinės išsišakojimą, kenkėjas turės atlikti darbą, kurį padarė visas tinklas nuo išsišakojimo pradžios iki eina-

[13] Paveikslėlyje pavaizduota architektūra yra prototipinė autoriaus sukurta blokų grandinė. Realybėje egzistuojančių blokų grandinių architektūros yra kur kas sudėtingesnės.

mojo momento [Nak+08]. Be to, atlikti PoW darbą reikės gerokai sparčiau nei visi kiti tinklo nariai kartu sudėjus, kad kenkėjas ne tik pasivytų visą tinklą grandinės ilgiu, bet ir jį aplenktų. Visa tai tam, kad kenkėjo sukurtas grandinės išsišakojimas taptų ilgesnis už pagrindinę grandį[14] [Nak+08]. Tik tokiu atveju piktybinę grandį tinklas priimtų kaip teisingą (žr. 7 pav.).

Šiuo metu tiek Bitcoin, tiek Ethereum toks scenarijus yra mažai tikėtinas, nes naujus blokus sukuria didelis kiekis kasėjų (angl. *Miners*), kuriems PoW suteikia stimulą (angl. *Incentive*) kasti, t.y. kurti naujus blokus. Tą lemia PoW skatinimo sistema: už kiekvieną iškastą bloką yra skiriamas apdovanojimas – kriptovaliuta (angl. *Cryptocurrency*) [Nak+08]. Taigi, tinklo kenkėjui beveik nėra šansų pakreipti konsensuso algoritmo savo naudai – to daryti tiesiog neapsimoka ir beveik neįmanoma techniškai. Šitaip užtikrinamas vienas iš reikalavimų – duomenų nekintamumas ir vienareikšmiškumas.




7 pav. Blokų grandinės šakos [ZXD+17]

#### 2.2.1.2. Blokų grandinės pralaidumas

Blokų grandinės pralaidumas (angl. *Throughput*) priklauso nuo daugelio faktorių. Visi šie faktoriai yra susiję su transakcijų gyvavimo ciklu. Bitcoin atveju transakcijų gyvavimo ciklas veikia tokiu principu [Nak+08]:

1. Visų pirma, kiekvienas narys, sukurdamas transakciją, ją viešai paskelbia kitiems tinklo nariams tam, kad transakcija būtų įtraukta į bloką.
2. Bloko kasėjas surenka dalį arba visas viešai paskelbtas transakcijas į bloką ir atlieka darbą pagal PoW konsensuso algoritmą.
3. Apskaičiavęs darbo rezultatą kasėjas paskelbia naujai sukurtą bloką visiems tinklo nariams viešai.
4. Jeigu kiti tinklo nariai pasitiki bloke esančių transakcijų tinkamumu, blokas galiausiai prijungiamas prie visos grandinės pabaigos ir tinklas nuosekliai jungia naujus blokus prie šio

[14] Šis scenarijus dar yra vadinamas 51 procento ataka (angl. *51% Attack)* [Bal17].

bloko.

Tačiau tuo bloko gyvavimo ciklas nesibaigia. Jeigu blokas prijungiamas prie grandinės, dar nereiškia, kad jis laikomas patvirtintu. Tam, kad blokas būtų laikomas saugiai patvirtintu, o kartu su juo ir transakcijos jame, prie šio bloko nuosekliai dar turi būti prijungtas tam tikras kiekis blokų.

Taip pat yra tikimybė, kad transakcija nebus patvirtinta, jeigu blokų kasėjai jos neįtrauks į blokus. Blokų kasėjai renkasi transakcijas pagal tai, kokią jie naudą gaus pridėdami jas į bloką. Ši nauda matuojama transakcijos mokesčiu (angl. *Transaction fee*), kurį nurodo transakcijos kūrėjas. Taigi, gali atsitikti taip, kad, transakcijos kūrėjas pasiūlys per mažą kainą už savo transakcijos įtraukimą į bloką ir ji bus patvirtinta gerokai vėliau arba netgi niekada[15].

Taigi matome, kad transakcijų greitis priklauso nuo šių pagrindinių priežasčių:

- Mokesčio dydžio, kuris lemia, ar kasėjai bus linkę įtraukti transakciją į blokus ir kaip greitai ji bus įtraukta.
- Kiek blokas gali talpinti savyje transakcijų, arba kitaip bloko dydis baitais.
- Kiek laiko trunka bloko sukūrimas, kitaip – per kiek laiko atliekamas PoW skaičiavimas.
- Kiek reikalinga tolimesnių blokų, kad blokas būtų laikomas saugiai patvirtintu.

Žemiau pateikiama lentelė (žr. 1 lentelę) su Bitcoin ir Ethereum platformų rodiklių palyginimais[16]. Iš joje esančių duomenų seka maksimalus TPS greitis.

1 lentelė. Bitcoin ir Ethereum rodiklių palyginimas

| **Palyginimo kriterijus** | **Bitcoin** | **Ethereum** |
|---|---|---|
| **Transakcijų kiekis bloke** | Apie 4000 [ZGG+16] | 380 limitas[17] |
| **Bloko iškasimo laikas** | 10 min. [MTJ17] | 10-20 sekundžių [GKW+16] |
| **Patvirtinimo blokų skaičius** | 6 [XWS+17] | 12 [XWS+17] |
| **Saugaus patvirtinimo laikas** | 1 valanda [XWS+17] | 3 minutės [XWS+17] |
| **TPS limitas** | 7 TPS [MTJ17] | 25 TPS [BS18] |

[15] Scenarijus tikėtinas, jeigu transakcijų, laukiančių patvirtinimo, yra daugiau negu telpa viename bloke.

[16] Autorius nepateikia vidutinės transakcijos mokesčio kainos, nes kriptovaliutų kaina ir transakcijos mokestis rinkoje yra labai nepastovūs. Ethereum: https://ethgasstation.info, Bitcoin: https://bitcoinfees.info [žiūrėta 2019-05-17].

[17] Bloko GAS limitas – 8 mln. [HLC+18], o vienos transakcijos minimalus GAS limitas – 21 tūkst. [XWS+17]. Todėl 8000000 / 21000 = 380.

#### 2.2.1.3. Blokų grandinių trūkumai

1 lentelėje pateikti duomenys atskleidžia blokų grandinių trūkumus. Žinant tiekimo grandinių ir logistikos mastus, šiuo metu šios platformos turėtų rimtų sunkumų siekiant patenkinti rinkos poreikius dėl esamų technologinių suvaržymų:

- TPS limitai. Būtų sunku įsivaizduoti didelių sistemų funkcionavimą bent vienoje iš šių platformų, nes jos negalėtų susitvarkyti su milijoniniu transakcijų krūviu. Logistikoje yra įprasta, kad vien individualios siuntos kelionės gyvavimo cikle dažnai pasikeičiant savininkams, yra atliekama keletas ar net dešimtys transakcijų.
- Patvirtinimo laukimo laikas. Tiekimo grandinėse laikas yra svarbus ir kainuoja pinigus. Laukti kelioliką minučių ar net valandą, kol transakcija bus patvirtinta, stabdytų įprastą tiekimo grandinės tėkmę ir atneštų didelių nuostolių. Be to, naudojant blokų grandines egzistuoja tikimybė, kad transakcija taip ir nebus įtraukta į blokų grandinę ir ją teks atlikti iš naujo.
- Mokesčiai už atliekamas transakcijas tikriausiai yra vienas iš labiausiai atgrasančių suvaržymų. Tikėtina, kad tam tikrais atvejais mokesčiai už transakcijas gali būti aukštesni už transportuojamų prekių kainą.

Tam tikros blokų grandinės yra įgyvendinusios išmaniųjų kontraktų (angl. *Smart contracts*) funkcionalumą, kuris praturtina technologijos potencialą. Išmanusis kontraktas – programinis kodas, kuris vykdo komandas pagal prieš tai aprašytas taisykles [VB+14].

Ethereum išmanieji kontraktai įgalina automatizuotus kriptovaliutų pervedimus pagal programinį kodą, remiantis užprogramuotais scenarijais. Tačiau jų realizavimas praktikoje kol kas atrodo neefektyvus. Visi tinklo nariai, norintys patikrinti bloko validumą, turintį savyje transakciją, kuri inicijuoja išmaniojo kontrakto vykdymą, turi vykdyti tą patį išmaniojo kontrakto kodą [VB+14]. Dėl šios priežasties vienos decentralizuotos programėlės (angl. *Decentralized Application*), toliau - DApp, išpopuliarėjimas apkrovė ir smarkiai sulėtino Ethereum tinklą[18].

[18] Informacija paimta iš: https://cryptovest.com/news/ethereum-loses-to-cryptokitties-network-remains-slow [žiūrėta 2019-05-17].

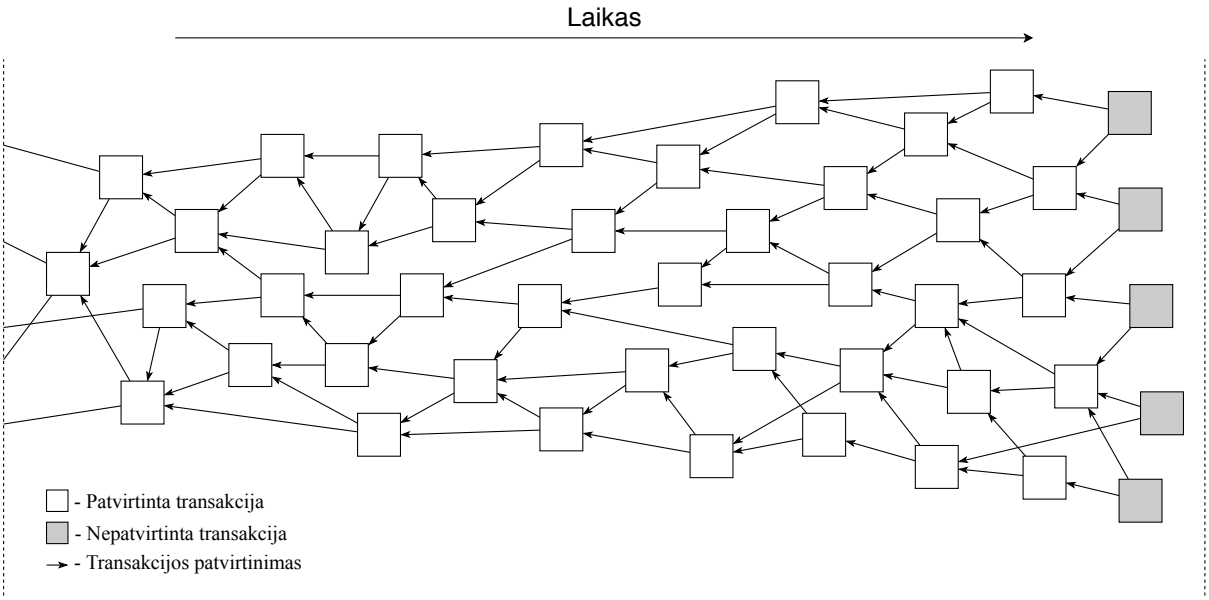
### 2.2.2. Orientuotas grafas be ciklų

Šiuo metu egzistuoja gerokai mažiau DAG principu paremtų projektų, negu jų yra blokų grandinių aplinkoje. Tačiau vienas iš įdomiausių ir daugiausiai žadančių – IOTA platforma.

#### 2.2.2.1. IOTA veikimo pobūdis

Vietoje blokų grandinės ir joje kasamų blokų su transakcijomis, IOTA įgyvendino DAG struktūrą turinčią išskirstytą transakcijų žurnalą, vadinamą raizginiu (angl. *Tangle*) (žr. 8 pav.). Modelyje vaidmenį atlieka 3 elementai:

- Patvirtinta transakcija. Tai tokia transakcija, kurią patvirtina bent viena kita transakcija.
- Nepatvirtinta transakcija. Jos dar vadinamos raizginio viršūnėmis (angl. *Tips*). Šios transakcijos jokia kita transakcija dar nepatvirtino.
- Transakcijos patvirtinimas. Kiekvienas IOTA tinklo narys, norėdamas atlikti transakciją, privalo patvirtinti kitas dvi transakcijas [Pop16].




8 pav. IOTA raizginio modelis [Pop16]

Transakcijų patvirtinimo įgyvendinimas yra unikalus ir specifinis procesas, kuriame didelę reikšmę turi matematiniai skaičiavimai. Visų pirma, norint atlikti transakciją IOTA tinkle, yra privaloma atlikti nuoseklius žingsnius: pasirinkti 2 transakcijas, patikrinti jų validumą ir atlikti darbą PoW principu [Pop16].

Unikalu yra tai, kad kiekvienas narys, norintis atlikti transakciją, PoW atlieka pats [Bra18]. Priešingai negu Bitcoin ar Ethereum, kur PoW galima deleguoti kitiems tinklo nariams, už tai

sumokant transakcijos mokestį. Tačiau IOTA naudojamas PoW yra gerokai paprastesnis ir nereikalaujantis daug skaičiavimo galios [Pop16]. Visų pirma, PoW reikalingas tam, kad būtų apsisaugoma nuo fiktyvių transakcijų (angl. *Spam*) [Pop16]. Skaičiavimų sudėtingumas žemas dėl to, kad IOTA pritaikyta daiktų internetui, kuriame dalyvauja labai smulkūs prietaisai, neturintys pajėgumų sudėtingiems skaičiavimams atlikti.

Tuo tarpu transakcijų parinkimo klausimas nėra toks trivialus ir nuo to priklauso visos ekosistemos stabilumas. IOTA ir neturi jokių formalių taisyklių transakcijų parinkimo patvirtinimui, t.y. galima laisva nuožiūra pasirinkti pačiam, kokias transakcijas patvirtinti [Pop16]. Tačiau egzistuoja rekomendacinis algoritmas [Pop16]. Šį algoritmą renkasi dauguma tinklo narių, nes sąžiningai jo laikantis padidėja tikimybė, kad likę nariai taip pat laikysis šio algoritmo. Iš to seka, kad algoritmo besilaikančių narių transakcijos bus patvirtintos kitų narių su aukštesne tikimybe.

2 transakcijos parenkamos pagal viršūnių parinkimo algoritmą (angl. *Tip Selection Algorithm*), toliau – TSA, o IOTA atveju konkrečiai – Markov Chain Monte Carlo (MCMC) algoritmu, kurio veikimui įtaką daro su kiekviena transakcija susieta informacija ir atributai [Bra18]. Tai transakcijos svoris (angl. *Weight*), transakcijos taškai (angl. *Score*) ir transakcijos kaupiamasis svoris (angl. *Cumulative Weight*) [Pop16].

#### 2.2.2.2. IOTA saugumas

IOTA platforma buvo pradėta kurti atsižvelgus į ateities perspektyvas ir kuriamas naujas technologijas. Viena iš tokių ateities perspektyvų – kvantiniai kompiuteriai (angl. *Quantum Computers*), kurie gali padaryti daugumą blokų grandinių pažeidžiamomis. Šis pažeidžiamumas kyla iš to, kaip yra atliekami PoW skaičiavimai ir kaip pasirašomos transakcijos [KPA+18]. Pakankamai galingas kvantinis kompiuteris galėtų įvykdyti 51 procento ataką ir pakreipti visą tinklą savo naudai [KPA+18].

Tai reiškia, kad Bitcoin, o kartu ir PoW konsensuso algoritmu paremtos blokų grandinės taptų nesaugios. Tačiau net jeigu blokų grandinė ir nėra paremta PoW konsensuso algoritmu, ji gali tapti nesaugi kitomis prasmėmis. Tam tikrais atvejais yra būtina paviešinti viešą raktą ir kvantinis kompiuteris, pasinaudojęs šiuo raktu, galėtų nustatyti privataus rakto reikšmę [ABL+17]. Privatus raktas yra naudojamas pasirašant transakcijas, patvirtinant savo tapatybę bei laikant kriptovaliutas (angl. *Cryptocurency*) kriptopiniginėse (angl. *Crypto Wallets*). Tokia spraga reikštų, kad asmenys, disponuojantys kvantiniu kompiuteriu, galėtų perskaityti privačiu raktu užšifruotas žinutes, pasisavinti sąskaitoje laikomą turtą ar apsimesti kitu asmeniu.

IOTA savo ruožtu nepateikia visiško atsparumo kvantinių kompiuterių atakoms, tačiau teigia, kad jų sprendimas yra žymiai saugesnis, negu Bitcoin ar kitų panašių platformų. IOTA naudoja Winternitz vienkartinę parašo panaudojimo schemą, kuri, kaip manoma, yra atspari kvantiniams kompiuteriams [EP18].

#### 2.2.2.3. IOTA pralaidumas

IOTA, priešingai negu blokų grandinės, neturi tokio architektūrinio vieneto kaip blokas, todėl pralaidumas ir greitis priklauso tik nuo individualių transakcijų patekimo į raizginį greičio. Žinant IOTA veikimo principą, galima išskirti rodiklius, darančius įtaką tinklo pralaidumui:

- PoW skaičiavimo, kurį atlieka transakciją kuriantis narys, atlikimo laikas;
- Kokia tikimybė, kad transakciją patvirtins kiti nariai;
- Kiek ilgai kitiems tinklo nariams užtrunka patikrinti transakcijos validumą ir ją patvirtinti;
- Kiek tinkle yra aktyvių narių, kuriančių transakcijas.

IOTA neturi konkrečių teorinių TPS limitų. Visi apribojimai kyla iš to, kaip greitai individualių transakcijų kūrėjai apskaičiuos kiekvienai transakcijai reikalingą atlikti PoW. Taip pat, kuo daugiau aktyvių narių tinkle, tuo aukštesnis bendras TPS dydis, nes daugiau narių kuria naujas transakcijas ir daugiau narių jas tvirtina. Taigi vieninteliai technologijos limitai – tai individualių mašinų tinkle kiekis bei jų skaičiavimo ir validavimo sparta.

Kitas svarbus aspektas – transakcijų mokestis. IOTA netaiko jokio transakcijų mokesčio [ZRS19]. O tai tampa pranašumu tinklo naudotojams, kurio neturi dauguma blokų grandinių naudotojų. Be to, transakcijos neprivalo perduoti kriptovaliutų. Tai reiškia, kad galima atlikti tuščias transakcijas arba tiesiog dalintis informacija su kitais tinklo nariais. Ši savybė tampa naudinga daiktų internete įrenginiams atliekant mikrotransakcijas.

#### 2.2.2.4. Maskuotieji nustatytos tapatybės pranešimai

Tiekimo grandinėse nepaprastai svarbus duomenų atsekamumas. Daugumai grandinės narių svarbu matyti prekės judėjimą, t.y. kur ir kada prekė keliavo, kaip pasikeitė prekės laikinieji savininkai, kokia buvo prekės būsena skirtingais laiko momentais ir t.t. Be to, kai kurie duomenys yra jautrūs ir reikia suvaldyti, kuri informacija kurioms šalims turi būti prieinama, o kuri – ne. Šį darbą dažnai tenka atlikti ranka, patikrinant skirtingus informacijos šaltinius.

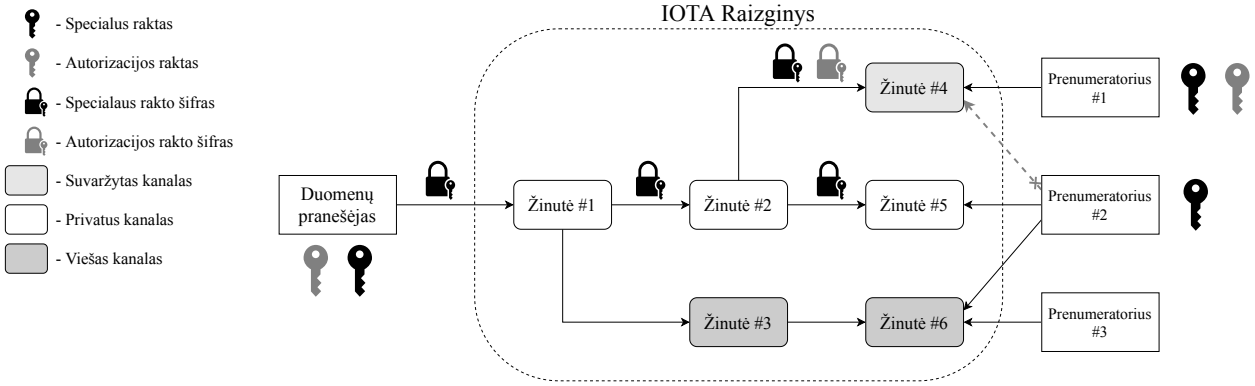
IOTA šiai problemai spręsti yra sukūrusi maskuotus nustatytos tapatybės pranešimus (angl. *Masked Authenticated Message*), toliau – MAM. Tai yra biblioteka, užšifruojanti, iššifruojanti ir

nustatanti tapatybę duomenų, kuriuos yra norima publikuoti į IOTA raizginį [Oso17]. Publikuojant tokius užšifruotus duomenis, galima atskleisti specialų raktą prenumeratoriams (angl. *Subscribers*), kurie turėtų teisę stebėti duomenis. Duomenų pranešėjas (angl. *Publisher*) tam sukuria kanalą (angl. *Channel*) [Mus18].

Kuriant kanalą atsiveria nemažai konfigūracijos pasirinkimų. Kanalą galima padaryti išsišakojusį, kiekvieną šaką padaryti prieinamą skirtingoms šalims ir kiekvienoje jų publikuoti skirtingą informaciją [Mus18]. Taip pat galima nustatyti norimą kanalo privatumo režimą iš 3 galimų rūšių [Han17]:

- Viešas (angl. *Public*), kuriame skelbiama informacija yra prieinama absoliučiai kiekvienam IOTA tinklo nariui.
- Privatus (angl. *Private*), kurį gali iššifruoti šalis, turinti specialų raktą. Naudinga įrenginių tarpusavio komunikacijai.
- Suvaržytas (angl. *Restricted*), kurį gali iššifruoti šalis, turinti specialų raktą, bei turinti autorizacijos raktą. Šis režimas leidžia kanalo iniciatoriui nutraukti transliavimą šalims, turinčioms tam tikrą autorizacijos raktą nepakeičiant specialaus rakto reikšmės. Nustačius naują autorizacijos raktą galima nustatyti, kam bus suteiktos naujos prenumeratorių teisės.

Supaprastintas MAM veikimo modelis pavaizduotas 9 pav. Duomenų pranešėjas siunčia žinutes, kurias stebi 3 prenumeratoriai. Pirmajam pranešėjas atskleidė specialų ir autorizacijos raktą, todėl jis gali iššifruoti ir perskaityti visų kanalų žinutes. Antrasis prenumeratorius turi specialų raktą, todėl gali skaityti privataus ir viešo kanalo žinutes, tačiau negali iššifruoti suvaržyto kanalo žinučių. Trečiasis prenumeratorius gali skaityti tik viešojo kanalo žinutes, t.y. trečią ir šeštą žinutes.




9 pav. MAM supaprastintas modelis

#### 2.2.2.5. Kvorumu paremti skaičiavimai

Kaip jau nagrinėta 2.2.1.3 poskyryje, išmanieji kontraktai praturtina blokų grandines. Ne išimtis ir IOTA. To pagrindu IOTA platformoje kaip atskiras sluoksnis yra kuriamas kvorumu paremtų skaičiavimų protokolas (angl. *Quorum Based Computations*), toliau – Qubic, sudarytas iš 3 esminių dedamųjų.

Pirmoji – orakulai (angl. *Oracles*), atliekantys tinklo tarpininko su išoriniu pasauliu vaidmenį [Fou19]. Galimas to pavyzdys – IOTA tinklas negali žinoti tiekimo grandinėse galimų rizikų, sukeltų gamtos stichijų ar kitų grandinės narių, kurių nemaža dalis aprašyta šaltiniuose [BAL+12; Str+13], poveikio ir dydžio. Orakulas šią informaciją galėtų surinkti ir transliuoti ją tinklui. Tačiau šia informacija orakulai gali manipuliuoti savo naudai. Kad to būtų išvengta, išorinio pasaulio faktų validumas turi būti priimtas kvalifikuota dauguma – kvorumu, t.y. ne mažiau nei 2/3 visų orakulų turi pateikti sutampančią informaciją [Fou19]. Taip pat egzistuoja ir kiti apsaugos mechanizmai, tokie kaip paskatos už teisingų rezultatų transliavimą, sankcijos už bandymus manipuliuoti informacija ir pan.

Antroji Qubic dedamoji – paskirstyti skaičiavimai [Fou19]. Daiktų internete smulkiems įrenginiams gali tekti susidurti su sudėtingais skaičiavimais, kurių šie įrenginiai nepajėgtų išspręsti arba tai užtruktų per daug laiko. Qubic protokolas įgalintų perduoti (angl. *Outsource*) šiuos skaičiavimus išorinėms ir gerokai galingesnėms mašinoms, kurios grąžintų skaičiavimų rezultatus smulkiems įrenginiams.

Paskutinė Qubic protokolo dalis – išmanieji kontraktai. Išmanieji kontraktai pasižymi savybe: žinodami, kokius įvesties duomenis paduosime kontraktui, taip pat žinosime, kokio rezultato iš jo tikėtis [Fou19]. Ši savybė leidžia juos pritaikyti realizuojant mašinų tarpusavio bendravimą (angl. Machine to Machine), toliau – M2M. Taip pat būtų galima automatizuoti informacijos apsikeitimą, bendravimą su prieš tai minėtais orakulais, bei paskirstytų skaičiavimų inicijavimą.

Qubic įgyvendinimas iš dalies yra panašus į turimos įtakos konsensuso algoritmą (angl. *Proof of Stake*), toliau – PoS, kurį turi įgyvendinę dalis blokų grandinių bei prie kurio ateityje ketina pereiti Ethereum platforma[19]. PoS efektyvina tinklo naudojamus resursus, likviduodama PoW atliekamą darbą mašinoms bei pašalindama globalaus konsensuso poreikį smulkiems dalykams. Taigi, vietoje to, kad validavimą, skaičiavimus bei balsavimą dėl visų išorinio pasaulio faktų atliktų kiekvienas tinkle esantis narys, šį darbą padaro orakulai.

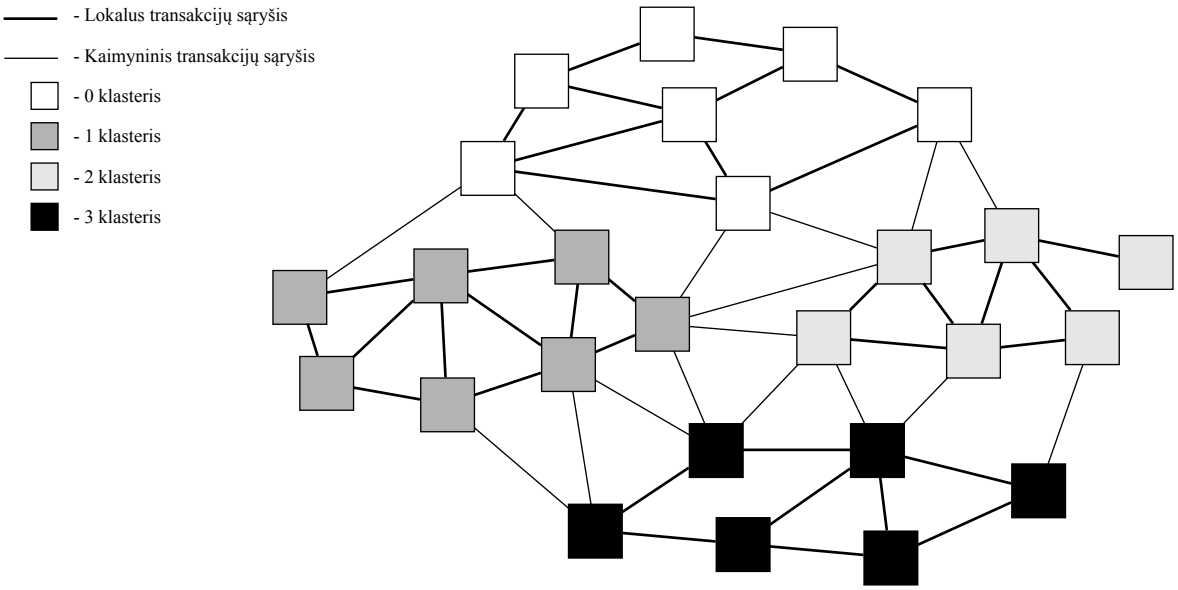
[19]Informacija iš: https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/proof-of-stake [žiūrėta 2019-05-17].

#### 2.2.2.6. Ekonominis klasterizavimas

Ekonominis klasterizavimas (angl. *Economic Clustering*), toliau EC – samprata, pristatyta Sergey Ivancheglo ir įgalinanti IOTA platformos plečiamumą, kitaip – neribotą TPS kiekį [Iva18]. Ekonominis klasteris – tai grupė prietaisų, esančių konkrečiame regione: kontinente, valstybėje, kelio ruože ar pastate [Iva18].

Pati idėja yra glaudžiai susijusi su daiktų internetu, o klasterių struktūra priklauso nuo ekonominės veiklos tame regione [Iva18]. IOTA platforma naudojasi vartotojai iš bet kurios pasaulio vietos, bet tai nėra efektyvu. Pavyzdžiui, JAV įsikūrusio fabriko temperatūros jutikliui nėra aktualu Kinijos piliečio transakcija savo draugui, gyvenančiam už kelių kvartalų. Tačiau jutiklis, norėdamas atlikdamas informacinę transakciją klientui, tikėtina, kad turės validuoti ir patvirtinti būtent jam neaktualią transakciją iš Kinijos. O juk būtų logiškiau, jeigu fabriko prietaisai turėtų prieigą tik prie jiems aktualių transakcijų ekonominiame regione.

EC išsidėstymo modelis pavaizduotas 10 pav. Kiekviename klasteryje yra lokaliai vykdomos IOTA transakcijos. Pavyzdžiui, 0 klasteris gali atlikti transakcijas 0 klasteryje, 1 klasteriui ir 2 klasteriui. Tačiau 0 ir 3 klasteris nėra kaimynai ir vienas kito transakcijų nemato, todėl jas ignoruoja. Jeigu iškiltų poreikis 0 klasterio nariui atlikti transakciją 3 klasteryje, šiam nariui tektų atlikti transakciją sau pačiam į 1 arba 2 klasterį, tada iš jo atlikti transakciją sau į 3 klasterį ir atlikti transakciją 3 klasteryje.




10 pav. Ekonominio klasterizavimo modelis

Tačiau iš EC modelio kyla tam tikri trūkumai ir rizikos [Iva18]:

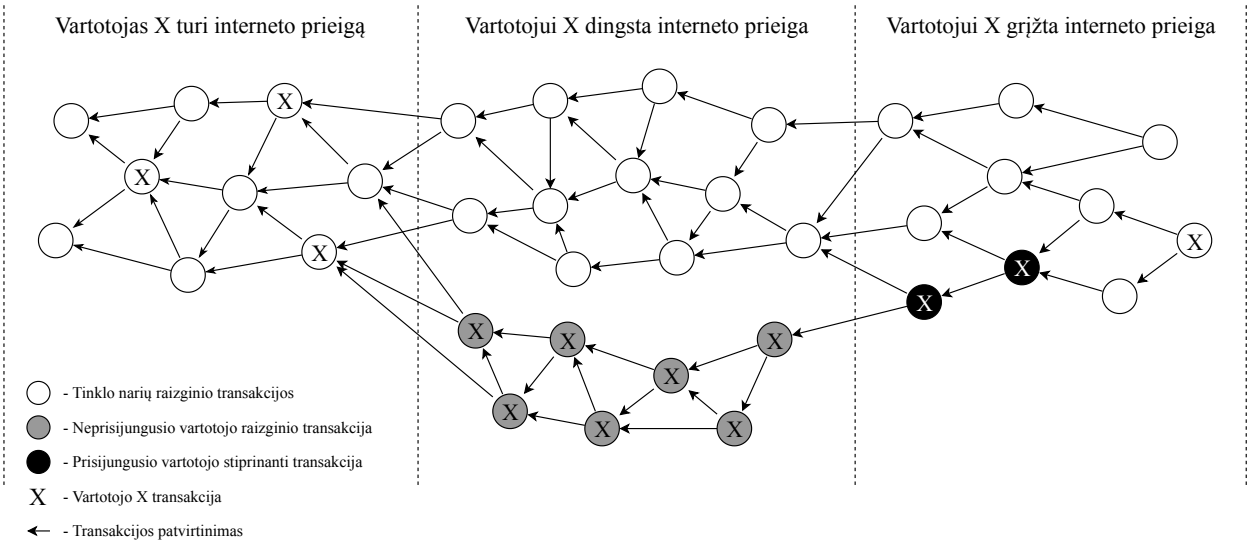
- Sunkumai atliekant transakcijas į tolimus klasterius;

- Dažnai tenka pervedinėti valiutą sau pačiam;
- Klasteriai gali kurti savo valiutą, kurios vertė kituose klasteriuose gali skirtis.

#### 2.2.2.7. Dalyvavimas tinkle neprisijungus

Transportuojant krovinius gali tekti atsidurti situacijose, kai interneto ryšys yra nepasiekimas. Svarbu, kad darbas tęstųsi net ir trumpam dingus internetui. Pavyzdys – krovinių plukdymas per vandenyną. Naudojama technologija turi užtikrinti stabilų veikimą be interneto, ir kad atsiradus interneto ryšiui nebūtų pateikiami suklastoti duomenys.

Šiuo klausimu IOTA yra pranašesnė už Bitcoin ir Ethereum, nes įgalina transakcijas neturint interneto ryšio [ZRS19]. Transakcijų vykdymas periode be interneto pavaizduotas 11 pav. Naudotojas X, dingus internetui, mato visas transakcijas, išskyrus tas, kurias likęs tinklas atlieka naudotojui X neturint interneto ryšio. Vienintelė logiška veiksmų seka naudotojui X yra susikurti savo atskirą raizginį (angl. *sub-tangle*), kuriame X transakcijos tvirtins X transakcijas.




11 pav. Transakcijų vykdymas neturint interneto prieigos

Atsiradus interneto prieigai dar nereiškia, kad vartotojo X atskiras raizginys bus patvirtintas, todėl reikia atlikti specialias stiprinančias transakcijas, kurios padidina šansus, kad tinklas palaipsniui pripažins ir validuos atskirą raizginį kaip tinkamą įtraukti į bendrą tinklą [Bre17]. Stiprinanti transakcija būtinai turi patvirtinti vieną pagrindinio raizginio ir vieną atskiro raizginio X transakciją [Bre17]. Kuo daugiau stiprinančių transakcijų, tuo didesnė validavimo tikimybė, tačiau yra reikalingos bent 2 stiprinančios transakcijos [Bre17].

## 2.3. Blokų grandinės ir orientuoto grafo be ciklų palyginimas

Taigi, galima apibendrinti pagrindinius skirtumus tarp DAG ir blokų grandinių principais paremtų DLT. Architektūra yra akivaizdžiausias skirtumas. Blokų grandinė yra tiesinės formos darinys, sudarytas iš nuosekliai sujungtų blokų, o DAG yra raizginys, sudarytas iš individualių transakcijų. Tačiau iš to kyla IOTA trūkumas – palankesnės sąlygos piktybinių transakcijų kūrimui. Blokų grandinėse sukurti atskirą piktybinių blokų atšaką yra gerokai sudėtingiau ir reikalauja daugiau resursų negu kuriant atskirą transakcijų grandį IOTA tinkle. Tačiau nuogąstauti dėl tinklo pažeidžiamumo nėra pagrindo. Tam, kad būtų pažeistas duomenų nekintamumas, abiem atvejais kenkėjo skaičiavimo resursai turi būti didesni nei viso likusio tinklo.

Abi DLT atmainos naudoja PoW skaičiavimus, tačiau IOTA tinkle kiekvienas narys juos atlieka individualiai. Tuo tarpu blokų grandinėse šį procesą galime deleguoti. Esant aukštam PoW skaičiavimų sudėtingumui, tai tampa trūkumu tiekimo grandinėse. Jeigu daiktų internetas taptų visuotinai naudojama technologija logistikoje, transakcijas arba apsikeitimą duomenimis turėtų atlikti net ir patys smulkiausi prietaisai, nepasižymintys didele skaičiavimo galia.

Dar vienas IOTA trūkumas yra koordinatorius. Šiuo metu pastaroji pltforma yra ankstyvoje fazėje ir negali savarankiškai funkcionuoti, todėl ją turi prižiūrėti specialus agentas, vadinamas koordinatoriumi [Bra18]. Yra teigiama, kad tai pažeidžia vieną iš pagrindinių DLT principų – nepriklausomumą nuo trečiųjų šalių. Šiuo atžvilgiu blokų grandinės lenkia IOTA, nes gali veikti autonomiškai, be trečiosios šalies įsikišimo. Vis dėlto IOTA kūrėjai ateityje tikisi pašalinti koordinatoriaus poreikį [Bra18].

Saugumo klausimu IOTA turi pranašumą kvantinių kompiuterių atžvilgiu, tačiau tai yra labiau aktualu ilgojoje perspektyvoje. Kol kas nėra sukurtų galingų, pigių ir plačiai naudojamų kvantinių kompiuterių, todėl šis privalumas šiandien nėra lemiamas veiksnys renkantis tarp šių dviejų DLT tipų. Be to, blokų grandinės laikui bėgant galėtų prisitaikyti prie kvantinių kompiuterių keliamų grėsmių pakeisdamos savo architektūrinius sprendimus.

Ko gero didžiausią įtaką technologijos pasirinkimui lemia rodikliai, susiję su atliekamų transakcijų greičiu ir kaina. Tiekimo grandinėms yra svarbu, kad transakcijos apsimokėtų, t.y. įvyktų kuo greičiau ir pigiau. Svarbu lyginti rodiklius, darančius įtaką maksimaliai tinklo apkrovai, vienos transakcijos įvykdymo laikui ir finansinei naudai. Didžioji dalis blokų grandinių turi TPS limitus arba transakcijos mokestį, o IOTA – ne. Taigi, pritaikius IOTA tiekimo grandinėse, būtų galima dalintis informacija už dyką ir labai greitai, sutaupant daug resursų visuose grandies procesuose.

IOTA taip pat įgalina transakcijas neprisijungus ir MAM, sukuriančius potencialių techno-

logijos panaudojimo atvejų, o pilnai įgyvendinus kvorumu paremtus skaičiavimus ir ekonominį klasterizavimą, jų atsirastų dar daugiau.

Nepaisant visų IOTA trūkumų, remiantis jos savybių ir rodiklių pranašumais blokų grandinių atžvilgiu bei sąlygomis daiktų internetui, galima teigti, jog būtent ši DLT atmaina yra palankesnė taikymui tiekimo grandinių ir logistikos srityje. Taigi, toliau pasirinkta konstruoti panaudojimo scenarijus tiekimo grandinės procesuose naudojant IOTA platformą.

# 3. IOTA platformos panaudojimas tiekimo grandinėse

## 3.1. Tiekimo grandinės atvejis

Tiekimo grandinės pavyzdinis atvejis buvo kuriamas šio darbo autoriaus, remiantis kelių šaltinių pavyzdinėmis idėjomis [Chr16; Har16; LCP17; WL09]. Naudojantis jomis buvo sukurta viena bendra diagrama (žr. priedą nr. 1).

Diagrama nebuvo siekiama pavaizduoti realaus pasaulio tiekimo grandinės pavyzdžio[20], o labiau siekta sukurti modelį, apimantį kuo daugiau skirtingų tiekimo grandinės fazių ir etapų, kad tai leistų geriau atskleisti IOTA platformos panaudojamumą. Pateiktas modelis galėjo būti dar detalesnis, tačiau tai nebūtinai atspindėtų norimos perteikti esmės.

Šis teikimo grandinės atvejis vaizduoja supaprastintą vaisių tiekimo grandinę nuo ūkininko, įsigyjančio sėklas iki kliento, perkančio vaisius prekybos centre. Tiekimo grandinė išskaidyta į 15 diskrečių etapų, kurių kiekvienas aprašytas atitinkamai.

**1. Ūkininkas superka sėklas iš tiekėjo.** Prieš tai yra sudaromas raštiškas kontraktas tarp sėklų tiekėjo ir ūkininko, kad už tam tikrą kainą ūkininkas gaus tam tikrą kiekį sėklų. Be to, sutartyje gali būti papildomų sąlygų, jei sėklų tiekėjas laiku neturės sėklų arba jų kokybė neatitiks keliamų standartų.

**2. Ūkininkas nurenka pasėtą derlių.** Ūkininkas pasėja vaisių sėklas, sudaro tinkamas sąlygas jų auginimui ir atėjus laikui užaugintus vaisius nurenka ir sandėliuoja.

**3. Ūkininkas parduoda derlių supirkėjui.** Pardavimas vyksta pagal iš anksto sudarytą kontraktą. Ūkininkas įsipareigoja atėjus konkrečiam terminui parduoti supirkėjui atitinkamą kiekį vaisių, tenkinančių nustatytą kokybės standartą už atitinkamą kainą.

**4. Kurjeris pakrauna vaisius į sunkvežimį.** Supirkėjas samdo kurjerį iš logistikos įmonės, teikiančios transportavimo paslaugas. Supirkėjas gali šiam darbui paskirti ir savo darbuotojus, atsakingus už prekių transportavimą. Pirmuoju atveju būtų sudaromas kontraktas tarp supirkėjo ir logistikos įmonės, įsipareigojančios atgabenti nepažeistas prekes iki nustatyto termino.

**5. Vaisiai transportuojami iki fabriko.**

**6. Vaisiai apdirbami (pagaminami jų išvestiniai produktai) ir sandėliuojami.** Priklausomai nuo vaisių supirkėjo veiklos srities, jis gali vaisius paruošti pardavimui, pvz. apipurkšti cheminiu produktu, suteikiantį blizgumą ar atsparumą, taip pat apdirbti juos supjaustant, panaudojant kaip

[20] Dėl konfidencialumo priežasčių įmonės nėra linkusios skelbti oficialių savo tiekimo grandinių modelių.

sudedamąją dalį kituose produktuose ir t.t. Galutiniai produktai sandėliuojami fabriko patalpose, kol atvyks kurjeriai, atsakingi už prekių transportavimą į prekybos centrus. Su prekybos centrais yra pasirašomi kontraktai, nustatantys, kokius produktus už kokią kainą vaisių supirkėjas parduos prekybos centrui.

**7. Apdirbti vaisiai pakraunami į sunkvežimį.** Čia kurjeris gali būti samdomas tuo pačiu principu, kaip ir 4 etape.

**8. Vaisiai transportuojami į jūrų uostą.** Jūrų uostas pagal vidines taisykles perima konteinerį ir paruošia jį pakrovimui į laivą.

**9. Vaisių konteineriai pakraunami į krovininį laivą.**

**10. Krovininis laivas nuplaukia į kitą uostą.**

**11. Vaisių konteineriai iškraunami į sunkvežimius.** Tikėtina, kad kurjeris yra iš tos pačios logistikos kompanijos, kurios sunkvežimis nuvežė konteinerį į pirmąjį jūrų uostą.

**12. Sunkvežimiai išvežioja vaisius į skirtingas šalis.** Transportuojant vaisius yra pasiekiama kitos valstybės siena, kur kurjeris susiduria su muitine.

**13. Muitinėse patikrinami kroviniai.** Priklausomai nuo valstybės, už krovinio įvežimą į šalį gali būti taikomi skirtingi mokesčiai, o kroviniui taikomos skirtingos taisyklės ir standartai. Už atsiskaitymą su muitine yra atsakingas prekybos centras, norintis įsivežti prekes. Atlikus visas būtinas procedūras muitinė išduoda specialų leidimą.

**14. Vaisiai išvežiojami į prekybos centrus.**

**15. Vaisiai parduodami galutiniams pirkėjams.**

## 3.2. Tiekimo grandinės atvejis pritaikius IOTA platformą

Šiame skyriuje autorius pateikia pavyzdinius tiekimo grandinės modelius pritaikius IOTA platformos savybes. Kiekvienas papildytas panaudojimo atvejo etapas arba etapai aprašyti atskirai poskyriuose, pateikiant diagramą su kiekvienu etapo žingsnio detaliu aprašymu.

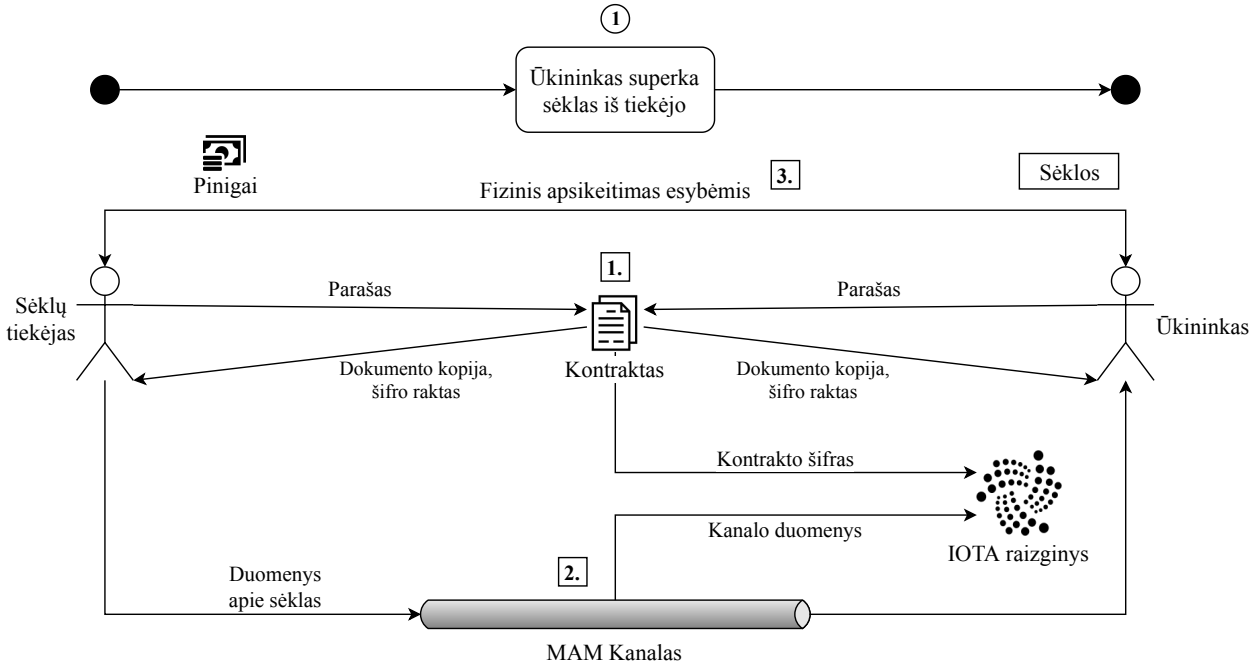
### 3.2.1. Pirmas etapas

Pirmojo etapo papildytas modelis, *Ūkininkas superka sėklas iš tiekėjo* (žr. 12 pav.):

1. Tarp sėklų pardavėjo ir ūkininko yra sudaromas kontraktas, kad už tam tikrą sumą tam tikru metu ūkininkas galės įsigyti tam tikrą kiekį sėklų. Kontraktas pasirašomas ūkininko ir sėklų

tiekėjo, o elektroninė sandorio versija užšifruojama raktu ir gautas šifras patalpinamas į IOTA raizginį. Abi šalys gauna dokumento kopiją ir šifro raktą. Niekas iš IOTA tinklo narių, išskyrus abi kontrakto šalis, negali peržiūrėti kontrakto turinio. Kontrakto šalys gali įrodyti turimos kontrakto kopijos autentiškumą užšifruodami šią kopiją ir patikrindami gauto šifro reikšmę su raizginyje esančiu šifru. Tai leidžia apsisaugoti nuo dokumentų padirbimo arba praradimo juos pametus.

2. Sėklų tiekėjas IOTA raizginyje sukuria MAM kanalą, kurį užsiprenumeruoja ūkininkas. Kanalas yra privatus, todėl sėklų tiekėjas prieš tai perduoda specialų raktą ūkininkui, kuris leidžia apsisaugoti, kad duomenų nematytų pašaliniai asmenys. Kanalu perduodami duomenys rašomi į raizginį, o ūkininkas realiu laiku gali stebėti sėklų būseną, pavyzdžiui lokaciją, sandėliavimo sąlygas ir pan.
3. Sėklų tiekėjas pristato sėklas ūkininkui, o ūkininkas atlieką finansinį pavedimą tiekėjui.




12 pav. 1 etapo papildytas modelis

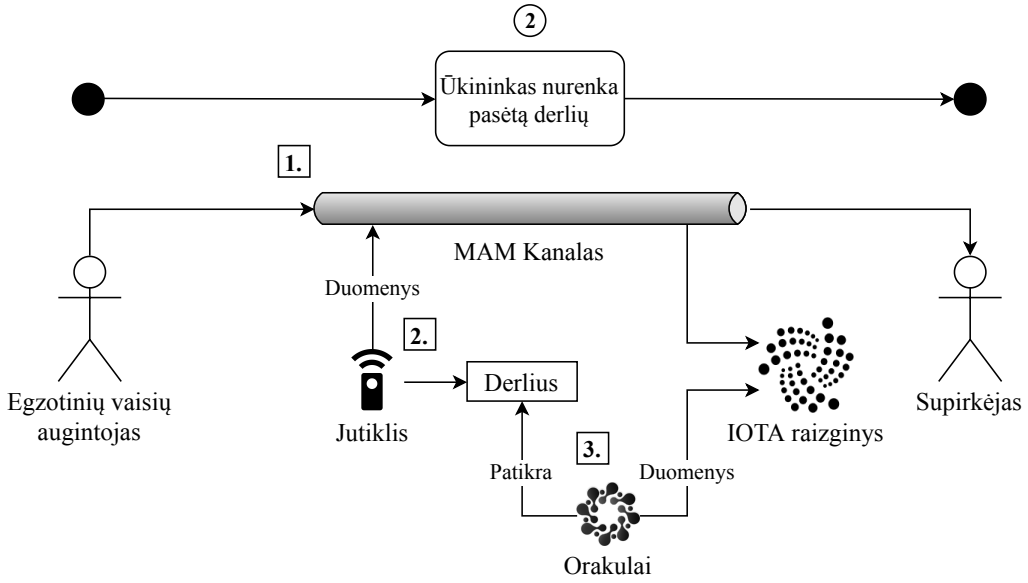
### 3.2.2. Antras etapas

Antrojo etapo papildytas modelis, *Ūkininkas nurenka pasėtą derlių* (žr. 13 pav.):

1. Iš pradžių ūkininkas inicijuoja privatų MAM kanalą, kuriuo siųs duomenis potencialiems derliaus supirkėjams. Ūkininkas perduoda kanalo prenumeratos raktą supirkėjui.
2. Ten, kur yra pasodintos sėklos, pastatomi jutikliai, renkantys duomenis apie aplinką. Šie jutikliai siunčia kanalu duomenis apie vaisių auginimo sąlygas: drėgmę, temperatūrą ir kt.

Jutiklius galima būtų sukonfigūruoti, kad kiekvienas atskirai siųstų duomenis į MAM kanalą, arba perduotų duomenis į ūkininko kompiuterį, kuris perimtų duomenų publikavimą.

3. Esant poreikiui, specialūs IOTA orakulų rolę prisiėmę inspektoriai gali atlikti patikrą, ar jutiklių siunčiami duomenys nėra klastojami ir savo matavimus taip pat patalpinti IOTA raizginyje. Specialūs orakulai galėtų prisidėti ir prie kitų reikalavimų laikymosi patikros. Pavyzdžiui, ar ūkininkas auginimo metu neteršia aplinkos, ar nėra darbinami vaikai ir t.t. Orakulai gali prisidėti ir prie draudimo įmonių veiklos. Esant sausrai ir ūkininkui nepristačius pakankamai derliaus, draudimo kompanijos, gavusios patvirtinimą iš orakulų apie stichinę nelaimę, galėtų padengti ūkininkų nuostolius. Orakulų turėtų dalyvauti kuo daugiau, šitaip užtikrinant, kad daugumos jų parodymai yra objektyvūs ir sutampa. Be orakulų būtų sunku nustatyti, ar jutiklių duomenys, kuriuos teikia ūkininkas, yra nepadirbti. Orakulas duomenis gali perduoti naudojant MAM kanalą.




13 pav. 2 etapo papildytas modelis

### 3.2.3. Trečias etapas

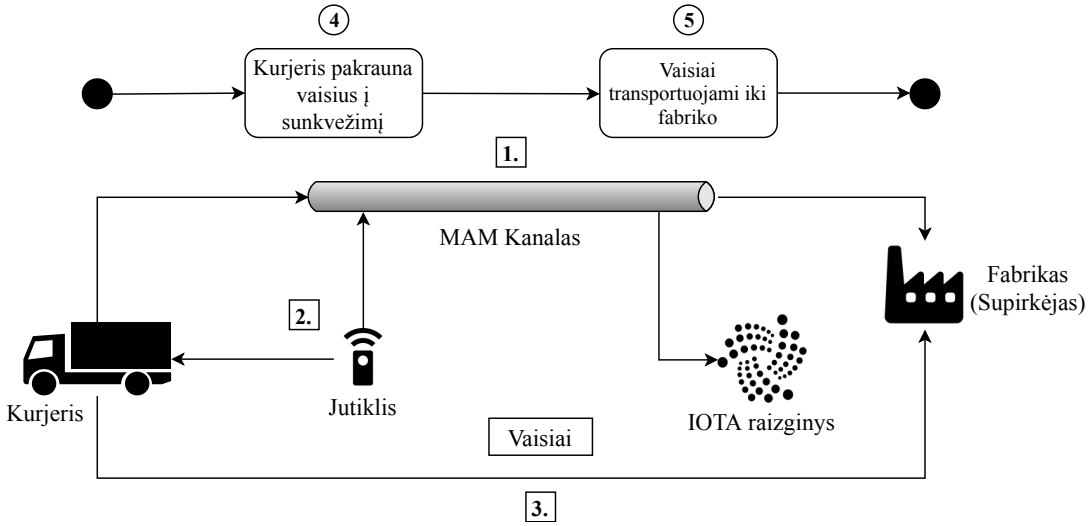
Trečiojo etapo, *Ūkininkas parduoda derlių supirkėjui* modelio papildymas yra beveik identiškas pirmojo etapo modelio papildymui. Šiuo atveju kontraktas tarp ūkininko ir supirkėjo gali būti sudaromas prieš antrą, o esant poreikiui, ir prieš pirmą etapą tam, kad būtų galima lengviau sekti įsipareigojimų vykdymą.

Svarbu pabrėžti, kad sutarčių ir kontraktų gali būti daugiau nei vienas. Į IOTA tinklą tiekimo grandinės nariai gali įkelti neribotą kiekį bet kokio tipo reikalingų dokumentų.

### 3.2.4. Ketvirtas ir penktas etapai

Ketvirtojo ir penktojo etapų, *Kurjeris pakrauna vaisius į sunkvežimį* ir *Vaisiai transportuojami iki fabriko* bendras papildytas modelis (žr. 14 pav.):

1. Pakrovęs vaisius į sunkvežimį kurjeris sukuria MAM kanalą šitaip patvirtinantis perėmęs krovinį ir perimantis atsakomybę už jį[21]. MAM kanalą prenumeruoja fabrikas[22].
2. Į MAM kanalą yra perduodami duomenys iš aplinkos jutiklio apie sunkvežimyje esančio krovinio sąlygas ir sunkvežimio lokaciją. Fabrikui (supirkėjui) tai yra naudinga, nes fabrikas gali reaguoti į vaisių atvežimą, pasiruošti jam. Be to, jei vaisiai vėluotų, dingtų bei būtų pristatyti pažeisti arba neatitinkantys kokybės, būtų aišku, kur incidentas įvyko ir kas už tai yra atsakingas.
3. Vaisiai pristatomi į fabriką, kur yra perduodama atsakomybė už juos.




14 pav. 4 ir 5 etapų papildytas modelis

### 3.2.5. Šeštas etapas

Šeštojo etapo papildytas modelis, *Vaisiai apdirbami (pagaminami jų sub-produktai) ir sandėliuojami* (žr. 15 pav.):

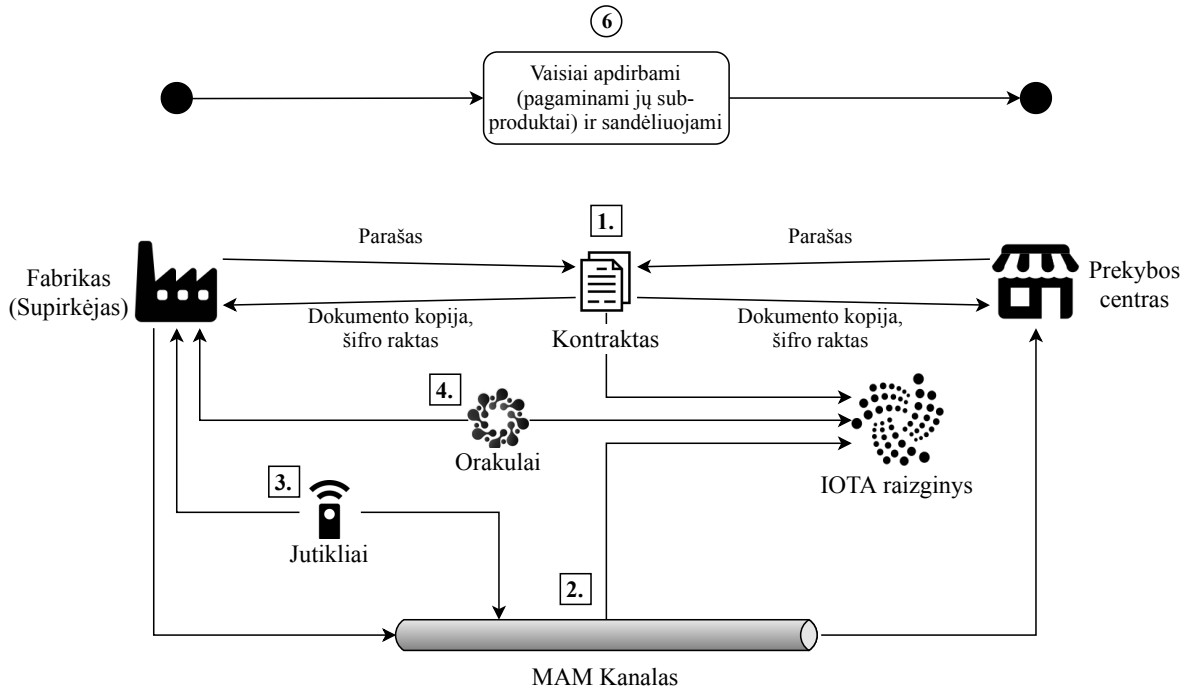
1. Kaip ir pirmajame panaudojimo atvejo etape, yra sudaromas kontraktas. Fabrikas (supirkėjas) susitaria su prekybos centru, kad už tam tikrą sumą tam tikru metu bus parduotas tam tikras kiekis perdirbtų arba paruoštų vaisių. Kontraktas pasirašomas abiejų šalių, o elektroni-

[21] Paprastai kaskart atlikus transakciją perduodant krovinį, kartu perduodama ir atsakomybė už jį. Tai reiškia, kad krovinį perimanti šalis turi patikrinti krovinio būklę ir su kroviniu susijusius dokumentus, kad būtų galima atrasti pažeidimo priežastį ir kaltininką.

[22] Šiame tiekimo grandinės pavyzdinio atvejo kontekste fabrikas priklauso supirkėjui.

nė versija užšifruojama raktu ir gautas šifras patalpinamas į IOTA tinklą [23]. Niekas iš IOTA tinklo narių, išskyrus abi kontrakto šalis, negali peržiūrėti kontrakto turinio. Kontrakto šalys gali įrodyti turimo kontrakto teisiškumą užšifruodami šią kopiją ir patikrindami gauto šifro reikšmę su raizginyje esančiu šifru.

2. Fabrikas sukuria privatų kanalą, kurį prenumeruoja prekybos centrai[24]. Kanalu fabrikas perduoda informaciją apie tai, kokie produktai kuriami, kurioje gamybos stadijoje šie produktai yra esamu laiko momentu, kokiais standartais vadovaujantis apdirbami ir t.t.
3. Fabrike įtaisyti jutikliai MAM kanalu taip pat perduoda informaciją, pavyzdžiui, gamybos sąlygas skirtinguose etapuose.
4. Esant poreikiui inspektoriai, kitaip orakulai, gali patikrinti tiek 2, tiek 3 žingsnyje fabriko teikiamą informaciją ir patalpinti į IOTA raizginį prekybos centrams pasitikrinti.




15 pav. 6 etapo papildytas modelis

### 3.2.6. Septintas ir aštuntas etapai

Septintojo ir Aštuntojo etapų, *Apdirbti vaisiai pakraunami į sunkvežimį* ir *Vaisiai transportuojami į jūrų uostą* bendras papildytas modelis yra beveik identiškas atitinkamai ketvirtojo ir penktojo etapų bendram papildytam modeliui. Kurjeriui sukūrus MAM kanalą, jį prenumeruoja ne tik prekybos centras, bet ir jūrų uostas, kad būtų pasiruošta sunkvežimio atvykimui.

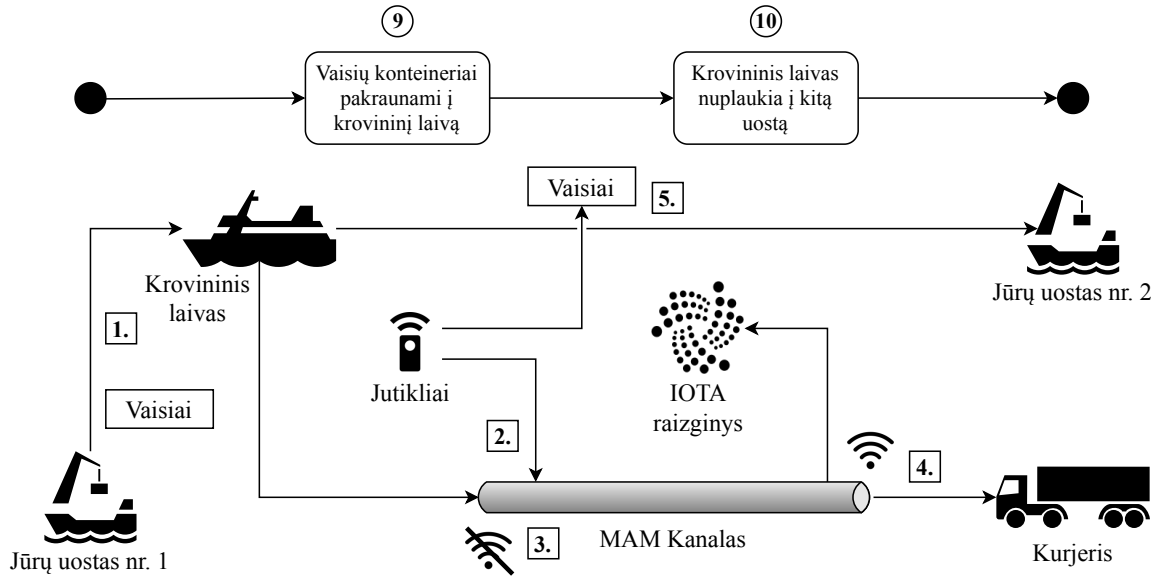
[23] Kontraktas gali būti sudarytas gerokai anksčiau, pavyzdžiui prieš 1 arba 2 etapą.

[24] Jeigu krovinius transportuoja samdomi kurjeriai iš logistikos įmonių, kanalu duomenys gali būti siunčiami ir šiems atstovams, t.y. koks krovinių tipas, kada krovinys paruoštas transportavimui ir t.t.

### 3.2.7. Devintas ir dešimtas etapai

Devintojo ir dešimtojo etapų, *Vaisių konteineriai pakraunami į krovininį laivą* ir *Krovininis laivas nuplaukia į kitą uostą* bendras papildytas modelis (žr. 16 pav.):

1. Vaisių konteineris pakraunamas į krovininį laivą.
2. Laivas sukuria MAM kanalą, kurį užprenumeruoja kurjeris, laukiantis krovinio jūrų uoste nr. 2. Kanalu perduodama konteinerio su vaisiais laikymo sąlygos, gaunamos iš jutiklių. Laivas išplaukia iš jūrų uosto nr. 1
3. Laivui plaukiant jūra, dingsta interneto ryšys, tačiau informacijos tiekimas nėra nutraukiamas ir informacijos transakcijos yra toliau atliekamos neprisijungus.
4. Po kiek laiko interneto ryšys grįžta ir visos iki tol siųstos žinutės atsiduria IOTA raizginyje, kurias prenumeruotojas gali gauti ir matyti iškart.
5. Vaisiai transportuojami į jūrų uostą nr. 2.

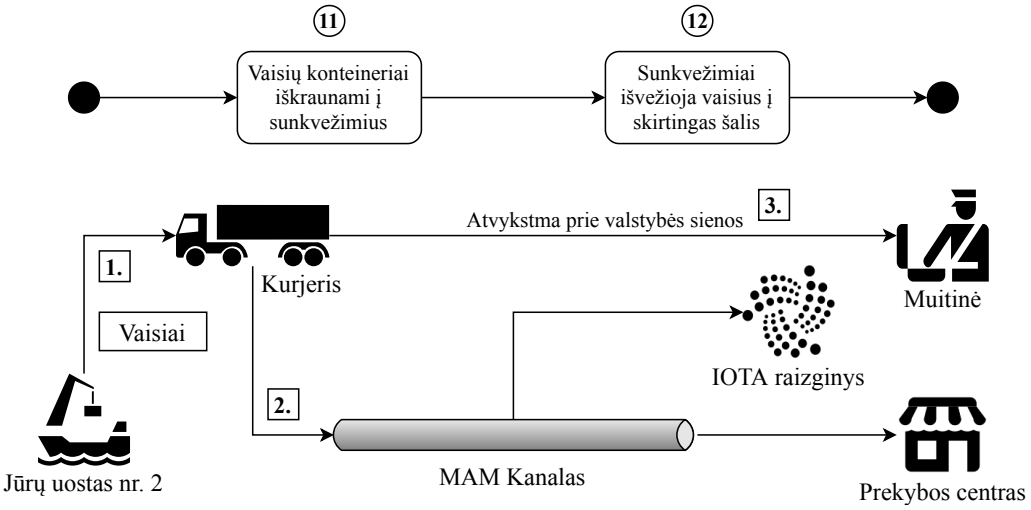



16 pav. 9 ir 10 etapų papildytas modelis

### 3.2.8. Vienuoliktas ir dvyliktas etapai

Vienuoliktojo ir dvyliktojo etapų, *Vaisių konteineriai iškraunami į sunkvežimius* ir *Sunkvežimiai išvežioja vaisius į skirtingas šalis* bendras papildytas modelis (žr. 17 pav.):

1. Jūrų uoste nr. 2 iškraunamas konteineris su vaisiais, kurį perima kurjeris.
2. Kurjeris sukuria MAM kanalą, kurį užprenumeruoja Prekybos centras.
3. Kurjeris galiausiai pasiekia kitos valstybės muitinę.

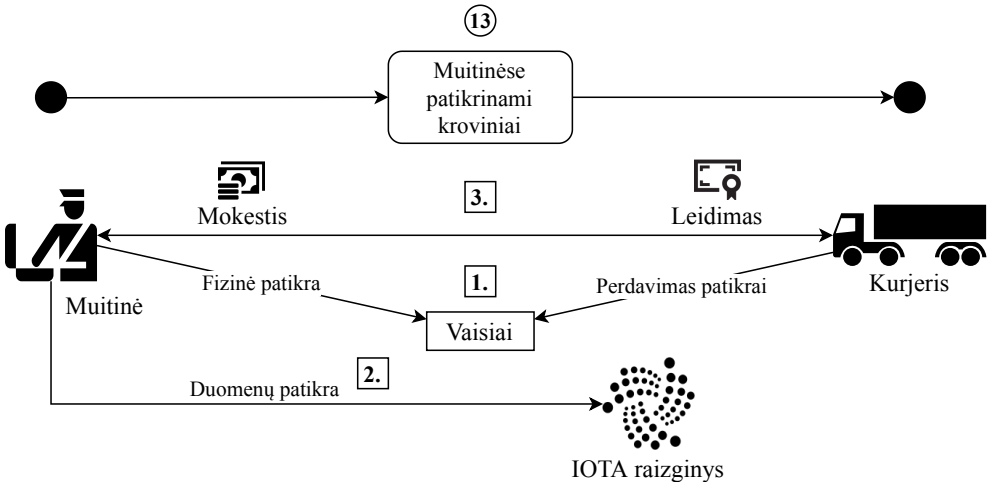



17 pav. 11 ir 12 etapų papildytas modelis

### 3.2.9. Tryliktas etapas

Tryliktojo etapo papildytas modelis, *Muitinėse patikrinami kroviniai* (žr. 18 pav.):

1. Kurjeris perduoda vaisių konteinerį muitinės darbuotojų patikrai.
2. Muitinės darbuotojai patikrina vaisių kelionės gyvavimo ciklo informaciją IOTA raizginyje. Ši informacija leidžia muitinės darbuotojams lengvai patikrinti svarbią informaciją. Pavyzdžiui, JAV pasienio muitų įstatymas įpareigoja pateikti krovinio pirkėją, pardavėją, gamintoją, kilmės šalį ir kitus duomenis [Pro18]. Visą šią informaciją būtų galima paprastai atsekti ir validuoti IOTA raizginyje, todėl tai galėtų sutaupyti daug laiko.
3. Muitinės darbuotojams neradus nieko įtartino, suteikiamas leidimas krovinį įvežti į valstybę. Leidimas taip pat gali būti įrašomas į IOTA raizginį. Vaisius transportuojantis atstovas susimoka muito mokestį (jeigu toks yra taikomas) ir toliau tęsia kelionę.

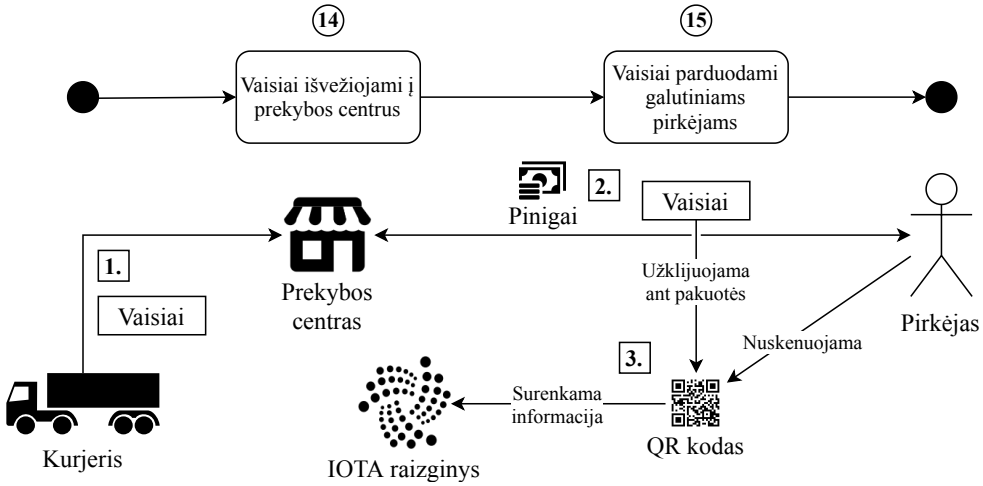



18 pav. 13 etapo papildytas modelis

### 3.2.10. Keturioliktas ir penkioliktas etapai

Keturioliktojo ir penkioliktojo etapų, *Vaisiai išvežiojami į prekybos centrus* ir *Vaisiai parduodami galutiniams pirkėjams* bendras papildytas modelis (žr. 19 pav.):

1. Vaisiai transportuojami į prekybos centrą, kuriame šie yra paruošiami pardavimui klientams. Ant vaisių pakuočių prekybos centras pagamina ir užklijuoja specialią informaciją savyje laikantį QR kodo lipduką.
2. Prekybos centrų klientai nusiperka vaisių pakuotes.
3. Pirkėjas gali įsitikinti prekybos centro pateikiama informacija, nuskenavęs ant pakuotės esantį QR kodą. Speciali programėlė galėtų leisti peržiūrėti kilmės šalį, vaisių kelionės maršrutą, vaisių auginimo, sandėliavimo ir transportavimo sąlygas, taip pat bet kokią papildomą informaciją, kurią tiekėjai gali atskleisti pirkėjui. Visa ši informacija gaunama iš IOTA raizginyje MAM kanalais bei kitais būdais patalpintos informacijos. Panašiais arba identiškais kodais gali būti žymimi kroviniai visuose tiekimo grandinės etapuose. Pasroviui esantys tiekimo grandinės nariai, prisijungę prie sistemos, galėtų nuskenuoti kodą ir matyti visą jiems aktualią informaciją.




19 pav. 14 ir 15 etapų papildytas modelis

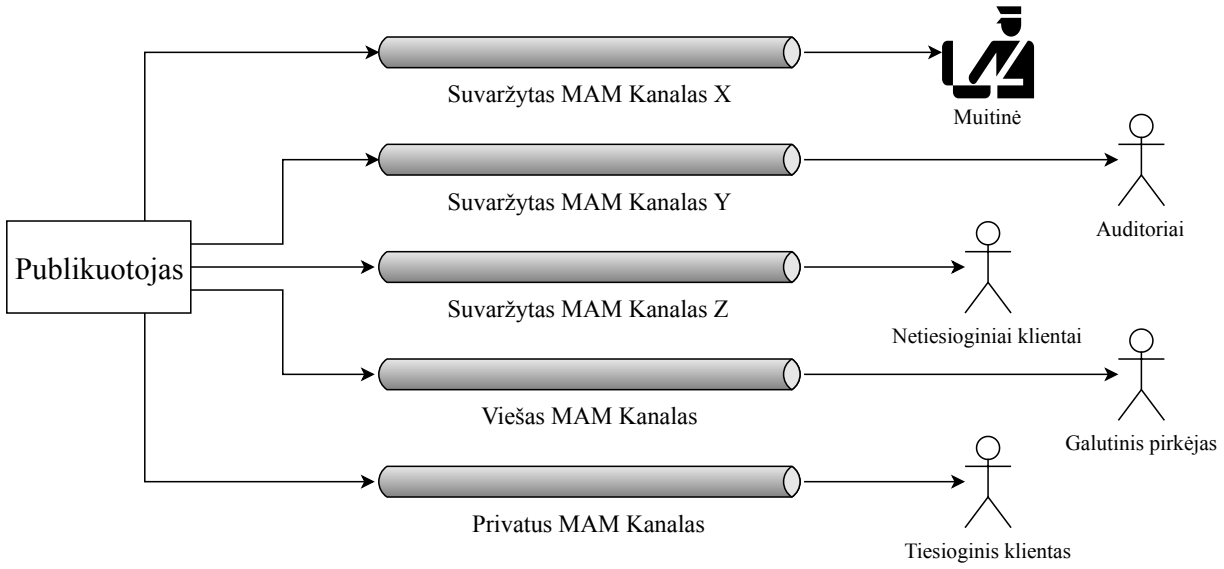
## 3.3. Alternatyvūs IOTA taikymai tiekimo grandinėje

3.2. poskyriuose buvo siūlomi IOTA platformos taikymo scenarijai pavyzdinėje tiekimo grandinėje. Tačiau įmanomos įvairios panaudojimo variacijos ir alternatyvos priklausomai nuo situacijos ir poreikio. Šioje dalyje bus nagrinėjamos kelios alternatyvos prieš tai pademonstruotiems panaudojimo atvejo etapų modeliams.

1-12 panaudojimo atvejo etapuose buvo naudojami MAM kanalai. Tačiau šie kanalai buvo sudaromi sukuriant prenumeratos teisę tik pasroviui esančiam tiekimo grandinės dalyviui. Kanalai buvo privatūs, kad informaciją būtų galima siųsti saugiai. Tačiau tiek galutiniai pirkėjai, tiek muitinės, neturėdamos specialaus rakto, gali peržiūrėti tik tą informacinį turinį, kurį pateikia prieš srovę esantis tiekėjas. Vienas iš sprendimo būdų būtų perduoti specialų MAM kanalo prenumeratos raktą visiems pasroviui esantiems tiekimo grandinės dalyviams.

Tačiau tai sukelia papildomų problemų. Skirtingų šalių yra daug: tiesioginiai klientai, netiesioginiai klientai, galutiniai pirkėjai, muitinės ir auditoriai. Visoms šalims reikalinga vis skirtinga informacija. Įmonė nenorėtų, kad konfidenciali informacija, skirta tiesioginiams klientams, pvz. transportavimo tvarkaraščiai arba turimas inventorius, būtų prieinamas galutiniams pirkėjams. Ir atvirkščiai, muitinėms, auditoriams ir galutiniams pirkėjams yra aktuali tik dalis informacijos iš viso srauto.

Naudojant skirtingus MAM kanalus skirstant informaciją tarp tiekimo grandinės šalių ir nustatant skirtingas prieigos teises, galima valdyti informacijos srautus (žr. 20 pav.). Kadangi tiesioginiai klientai keičiasi retai, sukuriamas jam skirtas privatus MAM kanalas. Suvaržytieji kanalai X, Y, ir Z perduoda skirtingus duomenis atitinkamiems prenumeruotojams. Kadangi tiek auditoriai, tiek muitinė, tiek netiesioginiai klientai gali dažnai kisti, yra parenkama suvaržyta kanalų apsauga, leidžianti dinamiškai keisti prenumeruotojus. Viešas kanalas yra skirtas galutiniams pirkėjams, tačiau duomenis gali peržiūrėti bet kas, turintis prieigą prie IOTA raizginio.

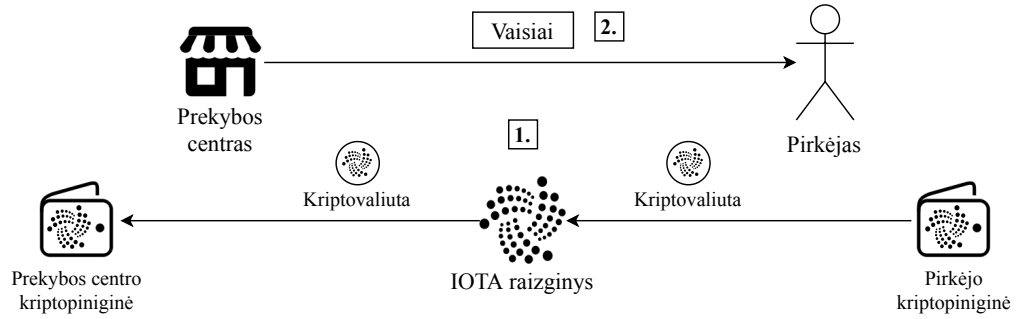



20 pav. Skirtingi MAM kanalų srautai

Pavyzdinio panaudojimo atvejo 1, 3, 13-15 etapuose ir bet kuriame kitame etape, kuriame vienas iš žingsnių yra finansinė transakcija, galima naudoti IOTA kaip atsiskaitymo terpę. Tokiam

scenarijui pavaizduoti yra tinkamas 3.2.10 poskyryje aprašomas 2 žingsnis. Šiuo atveju galutinis pirkėjas, t.y. prekybos centro klientas perka vaisių pakuotę, už kurią kasoje atsiskaito bankine kortele. Finansine transakcija pasirūpina bankas, o tai, kaip jau buvo minima 2 skyriuje, kelia įvairių rizikų.

Tačiau technologijai įsigalėjus klientas galėtų atsiskaityti kriptovaliuta IOTA raizginyje (žr. 21 pav.). Turėdamas savo kriptopiniginę[25], klientas pervestų kriptovaliutą į prekybos centro sąskaitą tiesiogiai ir ši transakcija būtų iškart įrašoma į IOTA raizginį. Tai reiškia, būtų išvengiama tarpininko, šiuo atveju banko. Tokie atsiskaitymai būtų galimi ir didesniais mastais, pavyzdžiui, milijoniniai finansiniai sandoriai tarp verslo šalių. Žinoma, tam reikėtų visuotinio technologijos ir kriptovaliutos pripažinimo ir nusistovėjimo, nes šiuo metu jos kaina labai svyruoja[26].




21 pav. Finansinė transakcija IOTA raizginyje

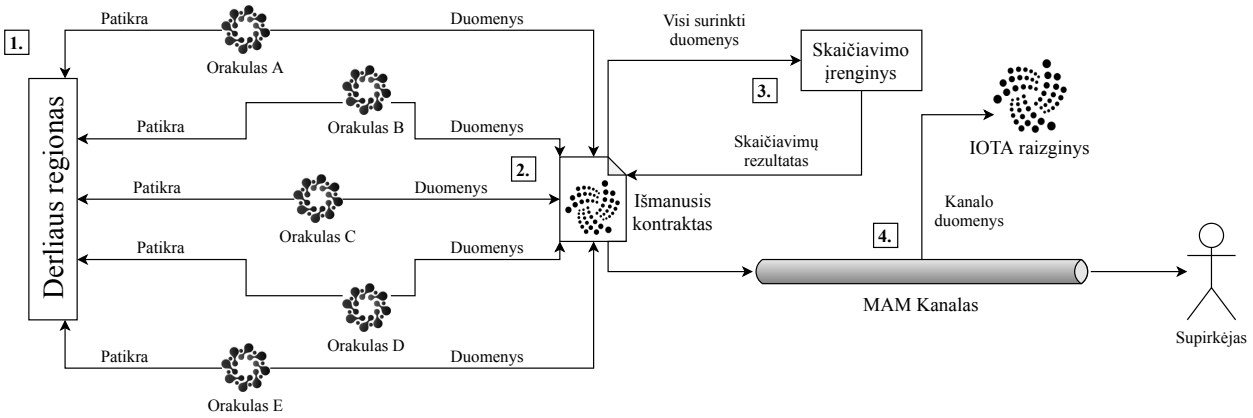
Pavyzdinio panaudojimo atvejo 2 etape svarbų vaidmenį vaidina orakulai, įrašydami savo duomenis į IOTA raizginį. Tai leidžia patikrinti, ar ūkininko pateikiami duomenys atitinka realybę. Tačiau 2 etapo 3 žingsnį galima praplėsti naudojant orakulus ir išmaniuosius kontraktus (žr. 22 pav.):

1. Geografiniame regione, kuriame ūkininkas augina vaisius, galėtų būti įsikūrę daugybė orakulų, kurie turėtų savo temperatūros matavimo prietaisus. Šiais prietaisais jie pamatuotų temperatūrą arba kitus rodiklius.
2. Kiekvienas orakulas perduotų savo duomenis išmaniajam kontraktui. Šioje vietoje įmanomas sandorio sudarymas tarp išmaniojo kontrakto savininko ir orakulų. Sandoris įpareigotų orakulus tiekti informaciją išmaniajam kontraktui už tam tikrą kriptovaliutos mokestį.
3. Išmanusis kontraktas surinktų visų orakulų duomenis ir juos visus perduotų išoriniam skaičiavimų įrenginiui. Atlikus skaičiavimus įrenginys grąžintų gautą skaičiavimų rezultatą išmaniajam kontraktui.

[25] Kruptopiniginėje yra laikomos kriptovaliutos. Šiame kontekste kriptopiniginė galėtų būti adresas IOTA raizginyje, kuriame saugomos kriptovaliutos.

[26] Duomenys iš: https://coinmarketcap.com [žiūrėta 2019-05-17].

4. Gautus galutinius skaičiavimus ir kitą informaciją išmanusis kontraktas perduotų MAM kanalu, kurį yra užsiprenumeravęs supirkėjas.




22 pav. Išmaniojo kontrakto ir orakulų bendradarbiavimas

## 3.4. Potencialios sistemos užduotys ir veiklos

Norint įgyvendinti IT sistemą, įgalinančią IOTA panaudojimą panašioje į tiekimo grandinę, pavaizduotą priede nr. 1, svarbu apsibrėžti sistemoje dalyvaujančias šalis, jų užduotis ir veiklas sistemoje. Remiantis 12-22 paveikslėliuose pavaizduotų siūlomų sprendimų modeliais, buvo surinktos esminės tiekimo grandinės veiklos, kurias galima įgyvendinti potencialioje sistemoje. Taip pat atrinkti visi tiekimo grandinėje esantys dalyviai. Gautas rezultatas pavaizduotas matricoje (žr. 2 lentelė).

2 lentelė. Skirtingų šalių dalyvavimo tiekimo grandinės procesuose matrica

| **Veikla** | **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** |
|---|---|---|---|---|---|---|---|---|---|---|
| Sudaryti sandorį | + | + | + | + | + | + | | + | + | |
| Patikrinti dokumento teisėtumą | + | + | + | + | + | + | + | + | + | |
| Sukurti MAM kanalą | + | + | + | + | + | + | + | | + | |
| Prenumeruoti MAM kanalą | | + | + | + | + | + | + | + | + | + |
| Siųsti kriptovaliutą | | + | + | | + | | | | + | + |
| Gauti kriptovaliutą | + | + | + | + | + | + | | + | + | + |
| Perduoti duomenis išmaniajam kontraktui | | | | | | + | | | | |
| Generuoti QR kodą | | + | + | + | + | | + | + | | |
| Nuskaityti QR kodą | | | + | + | + | | + | + | | + |

Lentelė reikalauja specialaus paaiškinimo. Kiekvienas stulpelio antraštės simbolis A-J reiškia vis skirtingą tiekimo grandinėje dalyvaujančią rolę. A – sėklų tiekėjas, B – ūkininkas, C – vaisių supirkėjas, D – kurjeris, E – prekybos centras, F – orakulas, G – muitininkas, H – jūrų uostas, I – išmaniojo kontrakto savininkas, J – galutinis pirkėjas. Langeliai su „+“ simboliu reiškia, kad atitinkama tiekimo grandinės šalis dalyvauja tam tikrame procese.

Autorius pastebi, kad potenciali sistema gali turėti daugybę kitų funkcionalumų, tokių kaip registracija, prisijungimas, istorijos peržiūra ir t.t. Tačiau šiame darbe nagrinėjamos pagrindinės bazinės sistemos veiklos, tiesiogiai susijusios su IOTA taikymo tiekimo grandinėje pavyzdžiais.

Dar vienas svarbus reikalavimas, kurį turi įgyvendinti sistema – tai nuolatinė prieiga prie IOTA raizginio. Tai yra būtina tam, kad sistemos ir raizginio duomenys visada būtų sinchronizuoti ir būtų remiamasi naujausia raizginio informacija. Tam užtikrinti reikalingas interneto ryšys. Nors, kaip jau minėta 2.2.2.7 ir 3.2.7 poskyriuose, tam tikrais atvejais sistema būtų galima naudotis ir neturint interneto prieigos.

Kiekviena 2 lentelėje pažymėta veikla turi būti prieinama atitinkamoms šalims per sistemos naudotojo sąsają naudotojui prisijungus. Tai reiškia, kad turi būti sukuriamos skirtingos sistemos būsenos priklausomai nuo to, koks naudotojas yra prisijungęs.

Tam, kad skaitytojui būtų paprasčiau įvertinti, ką ir kaip potenciali sistema turėtų atlikti, darbo autorius siūlo supaprastintus sistemos veiklų scenarijus, kuriems buvo nubraižytos panaudos atvejų ir veiklų UML diagramos. Visos diagramos buvo parengtos remiantis matricos duomenimis (žr. 2 lentelė) naudojant *draw.io* naršyklės įrankį.

Priede nr. 2 ir priede nr. 3 pavaizduotos sistemos užduočių diagramos, parodančios sistemos rolių (angl. *Actors*) galimas užduotis. Prieduose nr. 4-8 pavaizduotos veiklų diagramos, parodančios kaip ir kokiais scenarijais įvairios rolės ir sistema bendrauja tarpusavyje.

# Rezultatai

Darbo rezultatai:

1. Apžvelgta IOTA platforma kitų DLT platformų ir tiekimo grandinių keliamų reikalavimų kontekste;
2. Sumodeliuotas pavyzdinis tiekimo grandinės atvejis, sudarytas iš 15 diskrečių etapų;
3. Pasiūlyti IOTA taikymo pavyzdinėje tiekimo grandinėje sprendimų scenarijai kiekvienam etapui bei alternatyvos daliai jų;
4. Pateikti potencialios sistemos, įgyvendinančios IOTA pritaikymą tiekimo grandinėse, veikėjai, jų užduotys ir pagrindiniai veiklos scenarijai.

# Išvados

Darbo išvados:

1. Palyginus blokų grandinę ir orientuotą grafą be ciklų nustatyta, kad IOTA yra pranašesnė už kitas darbe nagrinėtas platformas tiekimo grandinėje, nes jos architektūra ir konsensuso mechanizmas įgalina nemokamas transakcijas bei likviduoja transakcijų per sekundę lubas;
2. Sukonstravus IOTA platformos taikymo scenarijų modelius pavyzdinėje tiekimo grandinėje buvo pastebėta, jog:
   2.1. IOTA platformą galima taikyti tiekimo grandinių procesuose;
   2.2. Qubic, MAM ir funkcionavimas neprisijungus yra tinkamos savybės taikymui tiekimo grandinėse;
   2.3. Esminė ir dažniausiai taikytina IOTA savybė tiekimo grandinėje yra MAM kanalai;
3. Kuriant potencialios sistemos užduotis ir veiklas pastebėta, kad:
   3.1. MAM kanalo prenumerata, dokumentų patikra ir kriptovaliutos gavimas yra dažniausiai naudojamos veiklos, nes kiekvieną iš jų vykdo 90% visų pavyzdinės tiekimo grandinės veikėjų;
   3.2. Prekybos centras ir supirkėjas turi daugiausiai veiklų ir atsakomybių sistemoje.

Autoriaus pateikiamos rekomendacijos:

1. Įgyvendinant potencialią sistemą būtų svarbu, kad viešą kanalą kurtų ir duomenis juo siųstų visi grandinės nariai. Tai padarytų duomenų prieinamumą galutiniam pirkėjui nuosekliu procesu;
2. Išmanųjį kontraktą būtų patogu traktuoti kaip patikimą vieną orakulą, jeigu jam duomenis siųstų keli orakulai;
3. Siekiant labiau decentralizuoti tinklą, išmaniojo kontrakto duomenų, gautų iš orakulų apdorojimą ir skaičiavimų rezultato pateikimą vertėtų perduoti taip pat tinklui. Vietoje vieno skaičiavimo įrenginio, darbus būtų galima deleguoti tinkle esantiems nariams, kuriems už suteikiamas paslaugas išmanusis kontraktas atsiskaitytų kriptovaliuta.

Taip pat pabrėžiamos kitos su darbo tema susijusios ir galimos tolimesnės tyrinėjimų temos bei kryptys, kurių autorius šiame darbe nenagrinėjo arba nagrinėjo mažai:

1. IOTA platforma paremtos tiekimo grandinės valdymo sistemos kūrimas.
2. IOTA platforma paremtos ir tradicinių tiekimo grandinės valdymo sistemų palyginimas.

3. Ekonominio klasterizavimo įtaka IOTA tinklo greičiui ir atsparumui atakoms.
4. Mašinų tarpusavio bendravimo automatizavimas taikant IOTA platformą.

# Literatūra


[ABL+17] D. Aggarwal, G.K. Brennen, T. Lee, M. Santha ir M. Tomamichel. Quantum attacks on bitcoin, and how to protect against them. *arXiv preprint arXiv:1710.10377*, 2017.

[AM16] S.A. Abeyratne ir R.P. Monfared. Blockchain ready manufacturing supply chain using distributed ledger, 2016.

[Bac16] L. Backlund. A technical overview of distributed ledger technologies in the nordic capital market. 2016.

[BAL+12] B. Behdani, A. Adhitya, Z. Lukszo ir R. Srinivasan. How to handle disruptions in supply chains–an integrated framework and a review of literature, 2012.

[Bal17] A. Baliga. Understanding blockchain consensus models. *Persistent*. 2017.

[BC15] P. Bharati ir A. Chaudhury. Current status of technology adoption: micro, small and medium manufacturing firms in boston. *Communications of the ACM*, 49(10):88–93, 2015.

[BCG+10] E. Briano, C. Caballini, P. Giribone ir R. Revetria. Resiliency and vulnerability in short life cycle products' supply chains: a system dynamics model. *WSEAS Transactions on Systems*, 9(4):327–337, 2010.

[Bra18] Q. Bramas. The stability and the security of the tangle, 2018.

[Bre17] B. Breier. *Technical Analysis of the Tangle in the IOTA-Environment*. Disertacija, Technical University of Munich, 2017.

[BS18] T. Bocek ir B. Stiller. Smart contracts – blockchains in the wings. *Digital Marketplaces Unleashed*, p. 169–184. Springer, 2018.

[CD05] R. Croson ir K. Donohue. Upstream versus downstream information and its impact on the bullwhip effect. *System Dynamics Review: The Journal of the System Dynamics Society*, 21(3):249–260, 2005.

[Chr16] M. Christopher. *Logistics & supply chain management*. Pearson UK, 2016.

[CV17] C. Cachin ir M. Vukolić. Blockchain consensus protocols in the wild. *arXiv preprint arXiv:1707.01873*, 2017.

[DD15] A. van Deursen ir J. van Dijk. Internet skill levels increase, but gaps widen: a longitudinal cross-sectional analysis (2010–2013) among the dutch population. *Information, Communication & Society*, 18(7):782–797, 2015.

[DHP17] A.J. Dweekat, G. Hwang ir J. Park. A supply chain performance measurement approach using the internet of things: toward more practical scpms. *Industrial Management & Data Systems*, 117(2):267–286, 2017.

[EP18] N. El Ioini ir C. Pahl. A review of distributed ledger technologies. *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, p. 277–288. Springer, 2018.

[Fer18] V. Ferrari. Eu blockchain observatory and forum workshop on gdpr, data policy and compliance. *Institute for Information Law Research Paper*, (2018-04), 2018.

[Fou19] IOTA Foundation. Qubic: quorum-based computations, 2019. Prieiga per internetą: <https://qubic.iota.org> [žiūrėta 2019-05-26].

[FW01] M.T. Frohlich ir R. Westbrook. Arcs of integration: an international study of supply chain strategies. *Journal of operations management*, 19(2):185–200, 2001.

[GKW+16] A. Gervais, G.O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf ir S. Capkun. On the security and performance of proof of work blockchains. *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, p. 3–16. ACM, 2016.

[GSS18] S.K. Garg, M.K. Sharma ir M. Shukla. It/is in supply chain management of agro industries. *Management of innovation, technology, transfer & flexibility for competitiveness in the globalized world. New Delhi, India: Global Institute of Flexible Systems Management*, 2018.

[GXC+18] Z. Gao, L. Xu, L. Chen, X. Zhao, Y. Lu ir W. Shi. Coc: a unified distributed ledger based supply chain management system. *Journal of Computer Science and Technology*, 33(2):237–248, 2018.

[Han17] P. Handy. Introducing masked authenticated messaging, 2017. Prieiga per internetą: <https://blog.iota.org/introducing-masked-authenticated-messaging-e55c1822d50e> [žiūrėta 2019-05-26].

[Har16] J. Hardy. Customer is king – the key element of a successful supply chain, 2016. Prieiga per internetą: <https://www.agric.wa.gov.au/newsletters/ovineobserver/ovineobserver-october-2016-76?page=0%2C2> [žiūrėta 2019-05-26].

[HLC+18] Y.C. Hu, T.T. Lee, D. Chatzopoulos ir P. Hui. Hierarchical interactions between ethereum smart contracts across testnets. *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, p. 7–12. ACM, 2018.

[HM07] N. Huber ir K. Michael. Vendor perceptions of how rfid can minimize product shrinkage in the retail supply chain. *2007 1st Annual RFID Eurasia*, p. 1–6. IEEE, 2007.

[HP16] J. Herrera-Joancomartí ir C. Pérez-Solà. Privacy in bitcoin transactions: new challenges from blockchain scalability solutions. *International Conference on Modeling Decisions for Artificial Intelligence*, p. 26–44. Springer, 2016.

[Iva18] S. Ivancheglo. Economic clustering and iota, 2018. Prieiga per internetą: <https://medium.com/@comefrombeyond/economic-clustering-and-iota-d3a77388900> [žiūrėta 2019-05-26].

[Jia17] J.H. Jiang. *How much does trust cost?: analysis of the consensus mechanism of distributed ledger technology and use-cases in securitization*. Disertacija, Massachusetts Institute of Technology, 2017.

[KGA+18] K. Kaur, S. Garg, G.S. Aujla, N. Kumar, J. Rodrigues ir M. Guizani. Edge computing in the industrial internet of things environment: software-defined-networks-based edge-cloud interplay. *IEEE communications magazine*, 56(2):44–51, 2018.

[KJ03] L.R. Kopczak ir M.E. Johnson. The supply-chain management effect. *MIT Sloan Management Review*, 44(3):27–34, 2003.

[KPA+18] E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, A.S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A.I. Lvovsky ir A.K. Fedorov. Quantum-secured blockchain. *Quantum Science and Technology*, 3(3):035004, 2018.

[LYH+18] J. Liu, F.R. Yu, Y. He, P. Si ir Y. Zhang. Virtualization for distributed ledger technology (vdlt). *IEEE Access*, 6:25019–25028, 2018.

[LCP17] P. Laurent, T. Chollet ir T. Pfeiffer. Continuous interconnected supply chain using blockchain and internet-of-things in supply chain traceability, 2017. Prieiga per internetą: <https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu-blockchain-internet-things-supply-chain-traceability.pdf> [žiūrėta 2019-05-26].

[MAS15] V. Mani, R. Agrawal ir V. Sharma. Supply chain social sustainability: a comparative case analysis in indian manufacturing industries. *Procedia-Social and Behavioral Sciences*, 189:234–251, 2015.

[MDK+01] J.T. Mentzer, W. DeWitt, J.S. Keebler, S. Min, N.W. Nix, C.D. Smith ir Z.G. Zacharia. Defining supply chain management. *Journal of Business logistics*, 22(2):1–25, 2001.

[MGM+11] A. Marucheck, N. Greis, C. Mena ir L. Cai. Product safety and security in the global supply chain: issues, challenges and research opportunities. *Journal of Operations Management*, 29(7-8):707–720, 2011.

[MLB+16] J. Manyika, S. Lund, J. Bughin, J.R. Woetzel, K. Stamenov ir D. Dhingra. *Digital globalization: The new era of global flows*, tom. 4. McKinsey Global Institute San Francisco, 2016.

[MR17] A.A. Majeed ir T.D. Rupasinghe. Internet of things (iot) embedded future supply chains for industry 4.0: an assessment from an erp-based fashion apparel and footwear industry. *International Journal of Supply Chain Management*, 6(1):25–40, 2017.

[MTJ17] M. Macdonald, L. Thorrold ir R. Julien. The blockchain: a comparison of platforms and their uses beyond bitcoin. *Work. Pap*:1–18, 2017.

[Mus18] A. Mushi. Iota: mam eloquently explained, 2018. Prieiga per internetą: <https://medium.com/coinmonks/iota-mam-eloquently-explained-d7505863b413> [žiūrėta 2019-05-26].

[Nak+08] S. Nakamoto ir k.t. Bitcoin: a peer-to-peer electronic cash system, 2008.

[Nil06] F. Nilsson. Logistics management in practice–towards theories of complex logistics. *The International Journal of Logistics Management*, 17(1):38–54, 2006.

[NOB18] G. Neubert, Y. Ouzrout ir A. Bouras. Collaboration and integration through information technologies in supply chains. *arXiv preprint arXiv:1811.01688*, 2018.

[ÖÇ16] E. Özcan ir M.A. Çimtay. Software application in supply chain management and examining of productivity effects of use “erp” in enterprises. *LM-SCM 2016 XIV. International Logistics and Supply Chain Congress*, p. 402, 2016.

[Oso17] A. Osowski. Masked authentication messaging, 2017. Prieiga per internetą: <https://github.com/iotaledger/MAM> [žiūrėta 2019-05-26].

[ØUJ17] S. Ølnes, J. Ubacht ir M. Janssen. Blockchain in government: benefits and implications of distributed ledger technology for information sharing, 2017.

[PMM+18] D. Puthal, N. Malik, S.P. Mohanty, E. Kougianos ir C. Yang. The blockchain as a decentralized security framework [future directions]. *IEEE Consumer Electronics Magazine*, 7(2):18–21, 2018.

[PO12] D. Prajogo ir J. Olhager. Supply chain integration and performance: the effects of long-term relationships, information technology and sharing, and logistics integration. *International Journal of Production Economics*, 135(1):514–522, 2012.

[Pop16] S. Popov. The tangle, 2016. Prieiga per internetą: <http://www.descryptions.com/Iota.pdf> [žiūrėta 2019-05-26].

[Pro18] U.S. Customs & Border Protection. Importer security filing and additional carrier requirements, 2018. Prieiga per internetą: <https://www.cbp.gov/sites/default/files/documents/import_sf_carry_3.pdf> [žiūrėta 2019-05-25].

[SP18] R.K. Shyamasundar ir V.T. Patil. Blockchain: the revolution in trust management. *Proceedings of the Indian National Science Academy*, 84(2):385–407, 2018.

[Str+13] M. Strom ir k.t. Pwc and the mit forum for supply chain innovation: making the right risk decisions to strengthen operations performance. pwc. MIT Forum for Supply Chain Innovation, 2013.

[VB+14] F. Vogelsteller, V. Buterin ir k.t. Ethereum whitepaper. *Ethereum Foundation*, 2014.

[VK06] S. Vachon ir R.D. Klassen. Extending green practices across the supply chain: the impact of upstream and downstream integration. *International Journal of Operations & Production Management*, 26(7):795–821, 2006.

[WL09] C.M. Webber ir P. Labaste. *Building competitiveness in Africa's agriculture: a guide to value chain concepts and applications*. The World Bank, 2009.

[XCS+17] L. Xu, L. Chen, N. Shah, Z. Gao, Y. Lu ir W. Shi. Dl-bac: distributed ledger based access control for web applications. *Proceedings of the 26th International Conference on World Wide Web Companion*, p. 1445–1450. International World Wide Web Conferences Steering Committee, 2017.

[XWS+17] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso ir P. Rimba. A taxonomy of blockchain-based systems for architecture design. *2017 IEEE International Conference on Software Architecture (ICSA)*, p. 243–252. IEEE, 2017.

[ZGG+16] Y. Zhu, R. Guo, G. Gan ir W.T. Tsai. Interactive incontestable signature for transactions confirmation in bitcoin blockchain. *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, tom. 1, p. 443–448. IEEE, 2016.

[ZM04] Z.G. Zacharia ir J.T. Mentzer. Logistics salience in a changing environment. *Journal of Business Logistics*, 25(1):187–210, 2004.

[ZN+15] G. Zyskind, O. Nathan ir k.t. Decentralizing privacy: using blockchain to protect personal data. *2015 IEEE Security and Privacy Workshops*, p. 180–184. IEEE, 2015.

[ZRS19] N. Zivic, C. Ruland ir J. Sassmannshausen. Distributed ledger technologies for m2m communications, 2019.

[ZXD+17] Z. Zheng, S. Xie, H. Dai, X. Chen ir H. Wang. An overview of blockchain technology: architecture, consensus, and future trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, p. 557–564. IEEE, 2017.

# Sąvokų apibrėžimai

**51% ataka** - vienas iš išskirstyto transakcijų žurnalo atakos būdų, kuomet kenkėjas bando turėti daugiau nei 50% viso tinklo pajėgumų ir šitaip jį užvaldyti.

**Atlikto darbo konsensuso algoritmas** - konsensuso algoritmas, paremtas dalyvavimu tinkle atliekant skaičiavimus.

**Bitcoin** - pirmoji blokų grandinės principu paremta platforma, pristatyta 2008 metais.

**Blokas** - blokų grandinių architektūrinis vienetas ir duomenų struktūra, laikanti savyje kitus duomenis.

**Blokų grandinė** - Viena iš išskirstytų transakcijų technologijos atmainų, kuri savyje laiko duomenis, tarpusavyje sujungtus į nuoseklių blokų seką.

**CRM** - ryšių su klientais valdymo sistema, padedanti organizuoti ir valdyti visos įmonės darbą, nukreiptą į esamų ir potencialių klientų poreikių patenkinimą.

**Decentralizuota programėlė** - programinis kodas, vykdomas išskirstytose sistemose.

**Dvigubo išleidimo problema** - potenciali spraga skaitmeninių pinigų sistemoje, kuomet tas pats piniginis vienetas gali būti išleistas ir priklausyti daugiau nei vienam asmeniui tuo pačiu metu.

**Ekonominis klasteris** - grupė IOTA tinklo narių, esančių tame pačiame regione.

**ERP** - programinė įranga, skirta kompiuterizuoti įmonės valdymą apjungiant duomenis ir procesus joje.

**Ethereum** - blokų grandinės principu paremta platforma, pirmą kartą pristatyta 2014 metais.

**GAS limitas** - Ethereum platformos vienetas, skirtas nusakyti, maksimalų GAS, kurį transakcijos kūrėjas yra linkęs išleisti už transakcijos patvirtinimą tinkle.

**GDPR reglamentas** - Europos Parlamento ir Europos Tarybos priimtas visoje ES tiesiogiai taikomas teisės aktas, įgyvendinantis asmens duomenų apsaugos reformą.

**IOTA** - orientuotų grafų be ciklų principu paremta platforma, pirmą kartą pristatyta 2015 metais.

**IOTA raizginys** - IOTA platformos tinklas, turintis savyje visas naudotojų transakcijas.

**Išmanusis kontraktas** - programinis kodas, automatiškai vykdantis komandas pagal prieš tai aprašytas taisykles.

**Išskirstyto transakcijų žurnalo technologija** - duomenų bazė, kuria konsensuso būdu dalinasi ir operuoja skirtingi naudotojai tinkle.

**Kasėjas** - asmuo, atliekantis skaičiavimus blokų grandinėse su tikslu sukurti bloką ir už tai gauti kriptovaliutos atlygį.

**Konsensuso algoritmas** - protokolas, kuris pasirūpina, kad visi tinklo nariai sinchronizuotųsi tar-

pusavyje ir prieitų bendrą sutarimą.

**Kriptopiniginė** – skaitmeninė piniginė, skirta kriptovaliutų siuntimui, gavimui ir laikymui.

**Kriptovaliuta** - skaitmeninis turtas, naudojamas išskirstytų transakcijų žurnalų transakcijose.

**Maišos reikšmė** - tam tikro ilgio skaitinė reikšmė, skirta identifikuoti unikalius duomenis.

**MAM kanalas** - specialus darinys IOTA tinkle, leidžiantis sukurti duomenų srautą, kurį gali prenumeruoti kiti asmenys tinkle.

**Markov Chain Monte Carlo algoritmas** - algoritmas, skirtas pasirinkti ir patvirtinti IOTA tinkle esančias viršūnes.

**Maskuotieji nustatytos tapatybės pranešimai** - biblioteka, užšifruojanti, iššifruojanti ir nustatanti tapatybę duomenų, kuriuos yra norima publikuoti į IOTA raizginį.

**Orakulas** - IOTA tinklo tarpininkas su išoriniu pasauliu.

**Orientuotas grafas be ciklų** - grafas, kurio visos briaunos turi kryptį ir savyje neturintis ciklų.

**Panaudos atvejo diagrama** - UML diagrama, apibūdinanti, ką projektuojama sistema gali atlikti, kartu aprašydama ir išorinius sistemos veikėjus.

**Qubic protokolas** - protokolas, veikiantis kaip atskiras IOTA sluoksnis, įgalinantis išmaniuosius kontraktus, orakulus ir išskirstytus skaičiavimus.

**Raizginio viršūnė** - IOTA raizginio transakcija, kurios nėra patvirtinusi jokia kita transakcija.

**RFID prietaisai** - priemonės, skirtos radijo dažnio bangų pagalba siųsti žinutes.

**Stiprinanti transakcija** - speciali transakcija IOTA tinkle, kuriama naudotojo savo paties transakcijų patvirtinimo tinkle tikimybei padidinti.

**TEU standartas** - standartinis vienetas, paremtas ISO 20 pėdų ilgio konteineriu ir naudojamas kaip statistinė eismo srauto ar mato priemonė.

**Tiekimo grandinė** - organizacijų, procesų, finansų, informacijos ir kitų esybių visuma, dalyvaujanti produkto gyvavimo cikle nuo pradinio tiekėjo iki galutinio kliento.

**Transakcijos kaupiamasis svoris** - IOTA transakcijos atributas, nusakantis šios transakcijos ir visų kitų transakcijų, tiesiogiai arba netiesiogiai patvirtinančių šią transakciją, svorių suma.

**Transakcijos per sekundę** - dydis, skirtas nusakyti, kiek transakcijų arba įrašų atsiduria transakcijų žurnale per sekundę.

**Transakcijos svoris** - IOTA transakcijos atributas, nusakantis, kiek tinklo naudotojas įdėjo pastangų sukurdamas transakciją.

**Transakcijos taškai** - IOTA transakcijos atributas, nusakantis visų tiesiogiai arba netiesiogiai šios transakcijos patvirtintų kitų transakcijų ir kartu šios transakcijos svorių sumą.

**Turimos įtakos konsensuso algoritmas** - konsensuso algoritmas, paremtas turimos įtakos tinkle, pavyzdžiu kriptovaliuta, disponavimu.

**Veiklų UML diagrama** - UML diagrama, aprašanti konkretaus scenarijaus vykdomus veiksmus.

**Viršūnių parinkimo algoritmas** - algoritmas, skirtas IOTA tinklo dalyviams atsirinkti transakcijas, kurios bus patvirtintos.

**Winternitz vienkartinė parašo panaudojimo schema** - kvantiniams kompiuteriams atspari schema, skirta generuoti viešus raktus IOTA tinkle.

# Santrumpos

**BVP** - Bendrasis vidaus produktas.

**CRM** - Klientų valdymo sistema (angl. *Customer Relationship Management*).

**DAG** - Orientuotas grafas be ciklų (angl. *Directed Acyclic Graph*).

**DApp** - Decentralizuota programėlė (angl. *Decentralized Application*).

**DLT** - Išskirstyto transakcijų žurnalo technologija (angl. *Distributed Ledger Technology*).

**EC** - Ekonominis klasteris (angl. *Ekonomic Cluster*).

**ERP** - Verslo valdymo sistema (angl. *Enterprise Resource Planning*).

**GDPR** - Bendrasis duomenų apsaugos reglamentas (angl. *General Data Protection Regulation*).

**JAV** - Jungtinės Amerikos Valstijos.

**M2M** - Mašinų tarpusavio bendravimas (angl. *Machine to Machine*).

**MAM** - Maskuotieji nustatytos tapatybės pranešimai (angl. *Masked Authentication Messaging*).

**MCMC** - Markovo grandinės Monte Karlo algoritmas (angl. *Markov Chain Monte Carlo*).

**PoS** - Turimos įtakos konsensuso algoritmas (angl. *Proof of Stake*).

**PoW** - Įdėto darbo konsensuso algoritmas (angl. *Proof of Work*).

**QR** - Greitas atsakas (angl. *Quick Response*).

**RFID** - Radijo dažnio identifikavimas (angl. *Radio-frequency identification*).

**TEU** - Dvidešimties pėdų vieneto ekvivalentas (angl. *Twenty-Foot Equivalent Unit*).

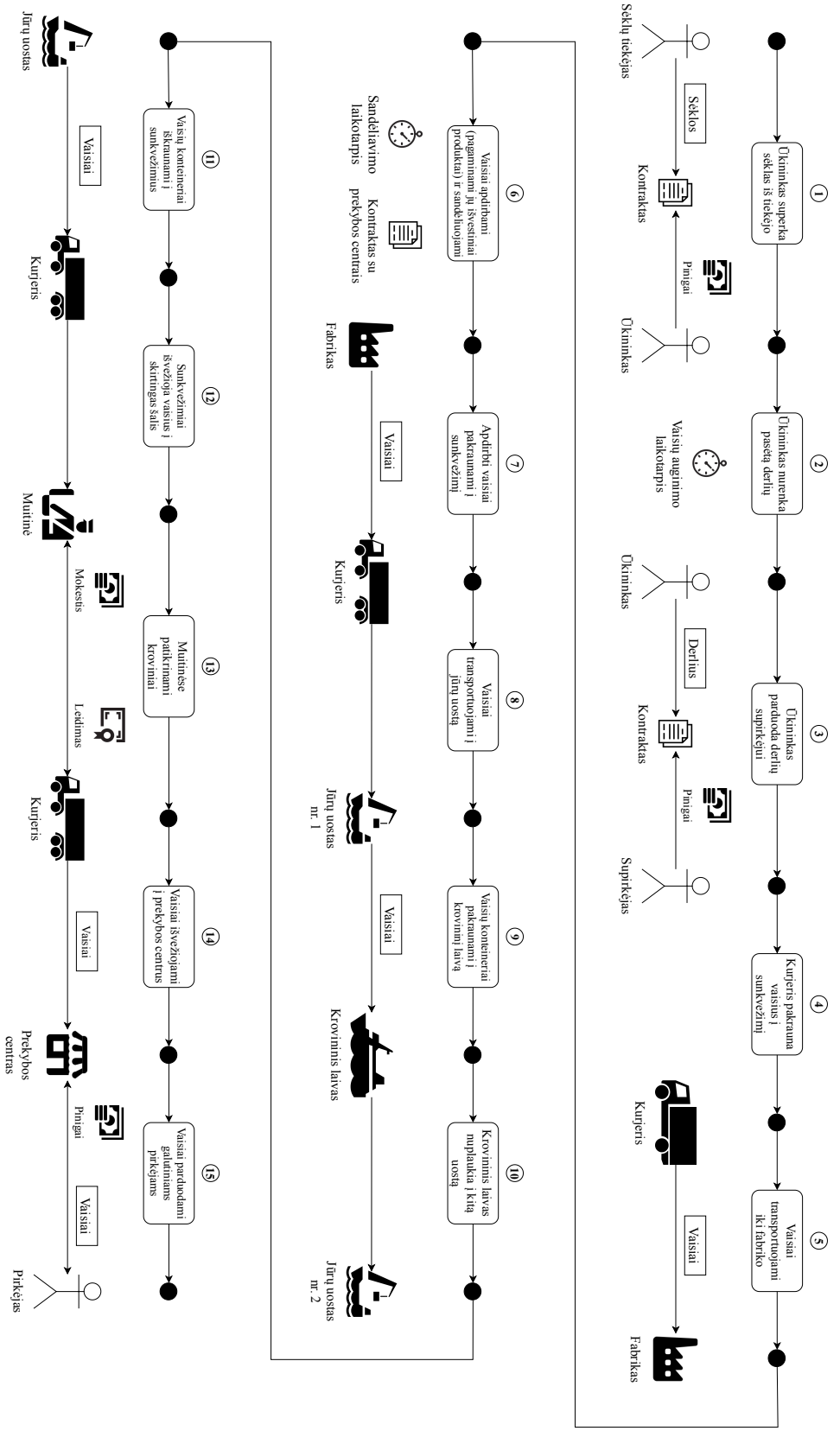
**TPS** - Transakcijų kiekis per sekundę (angl. *Transactions per Second*).

**TSA** - Viršūnių atrankos algoritmas (angl. *Tip Selection Algorithm*).

**UML** - Vieninga modeliavimo kalba (angl. *Unified Modeling Language*).

# Priedas nr. 1

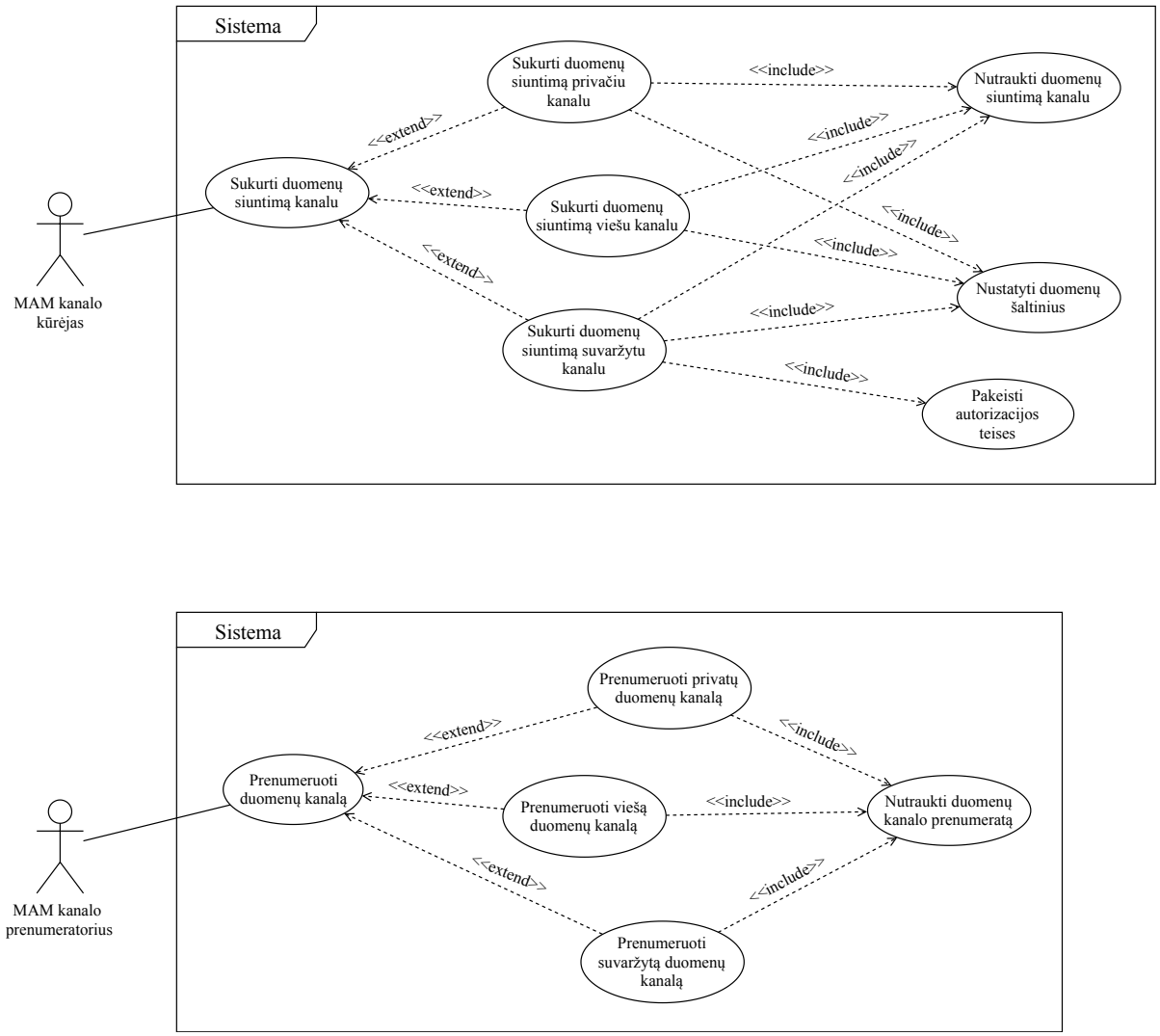
## Pavyzdinis tiekimo grandinės modelis (Vertikalus)




23 pav. Pavyzdinis tiekimo grandinės modelis (Vertikalus)

## Priedas nr. 2

## Maskuotųjų nustatytos tapatybės pranešimų kanalo kūrimo ir prenumeravimo panaudos atvejai



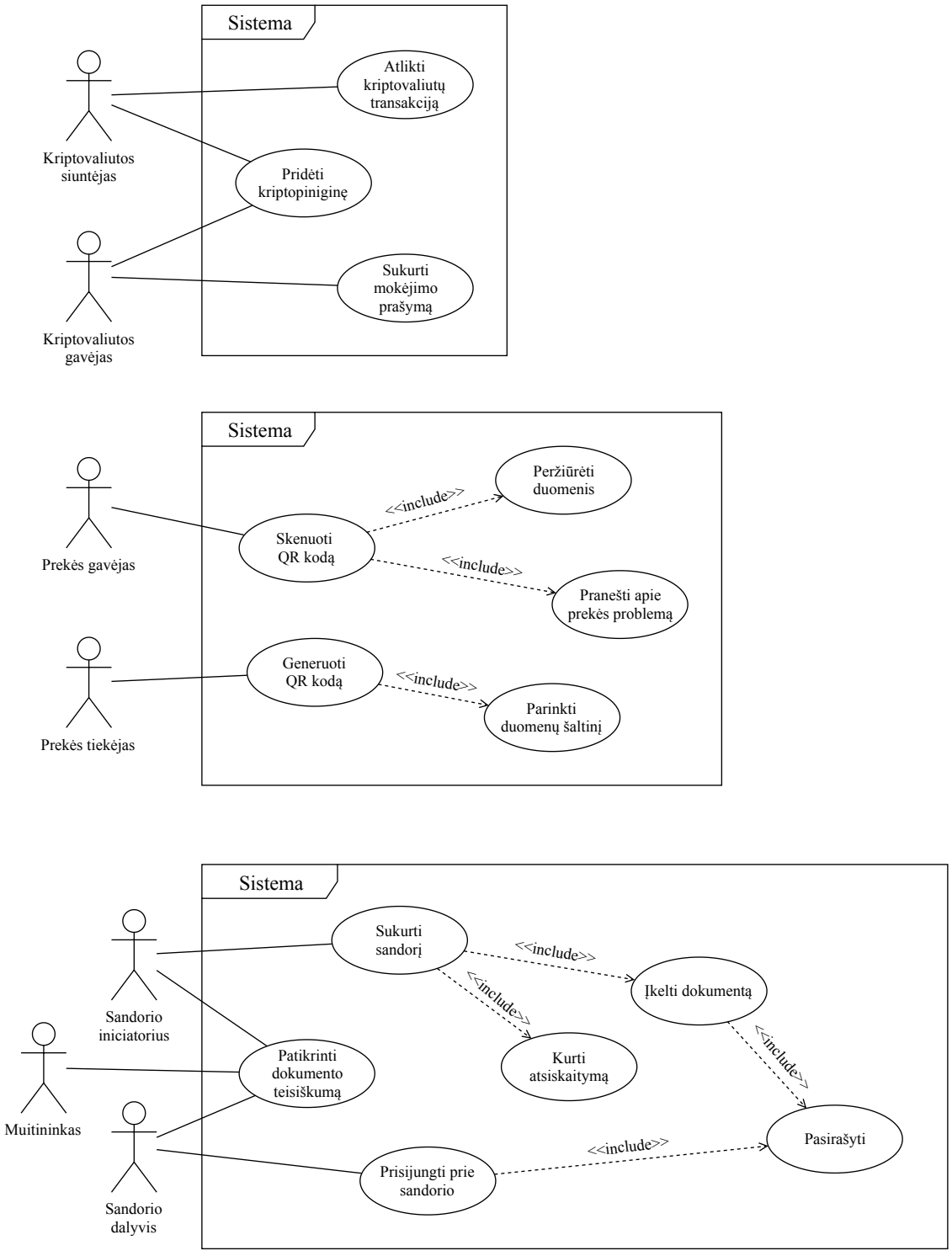




24 pav. MAM kanalo kūrimo ir prenumeravimo panaudos atvejai

## Priedas nr. 3

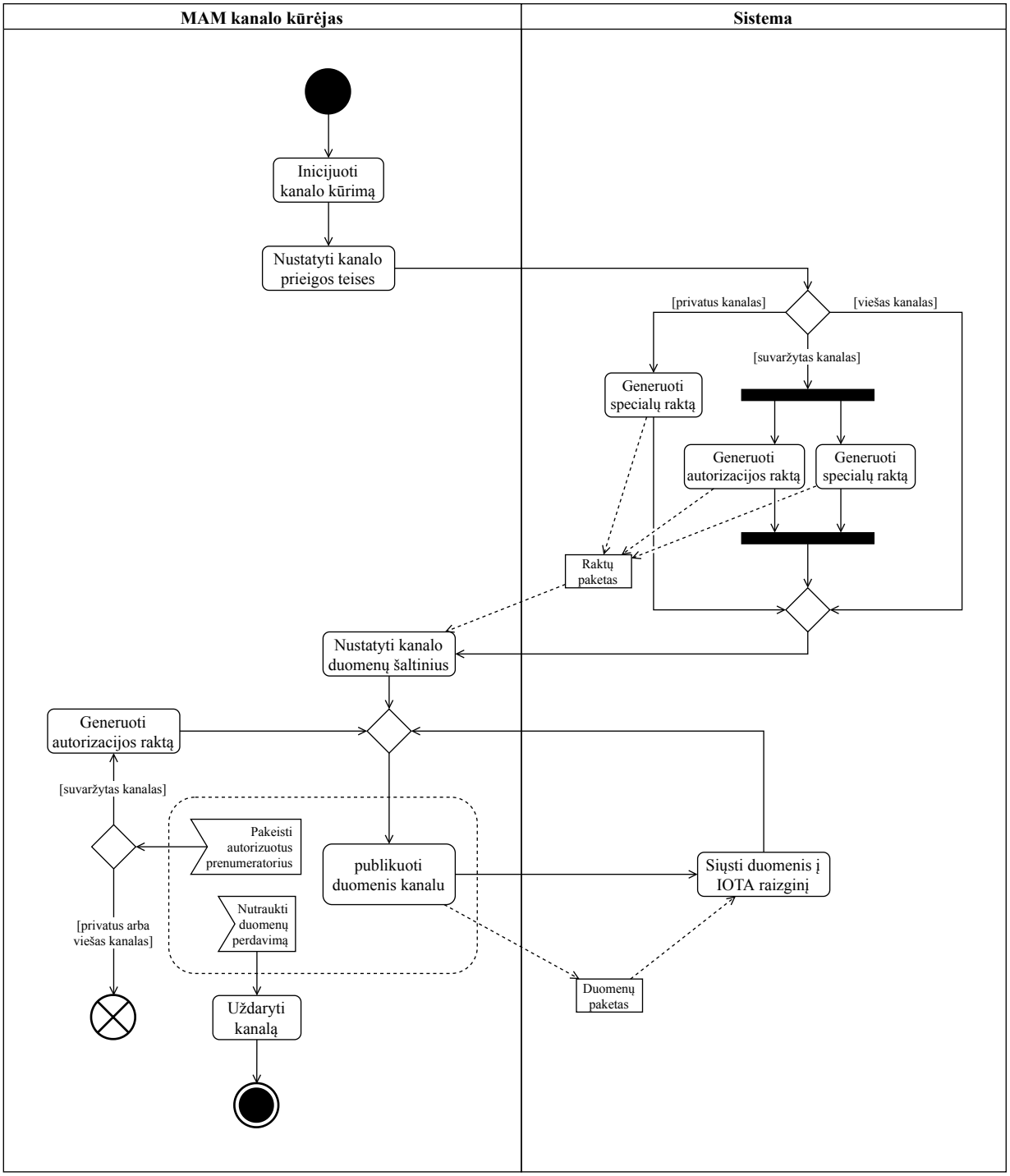
## Kriptovaliutų pervedimo ir gavimo, QR kodo generavimo ir nuskaitymo bei sandorio kūrimo panaudos atvejai




25 pav. Kriptovaliutų pervedimo ir gavimo, QR kodo generavimo ir nuskaitymo bei sandorio kūrimo panaudos atvejai

## Priedas nr. 4

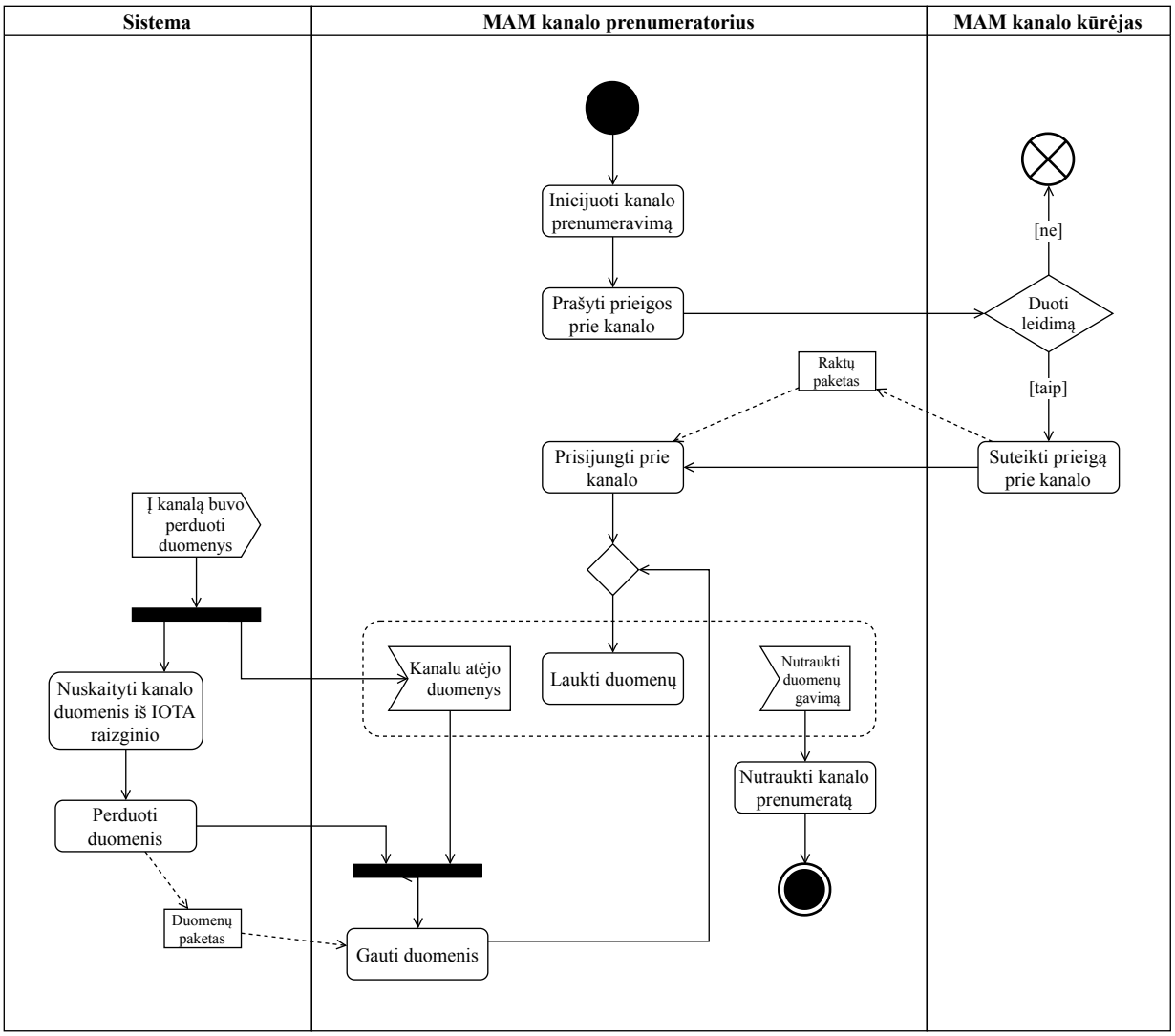
## Maskuotųjų nustatytos tapatybės pranešimų kanalo sukūrimo veiklų diagrama




26 pav. MAM kanalo sukūrimo veiklų diagrama

## Priedas nr. 5

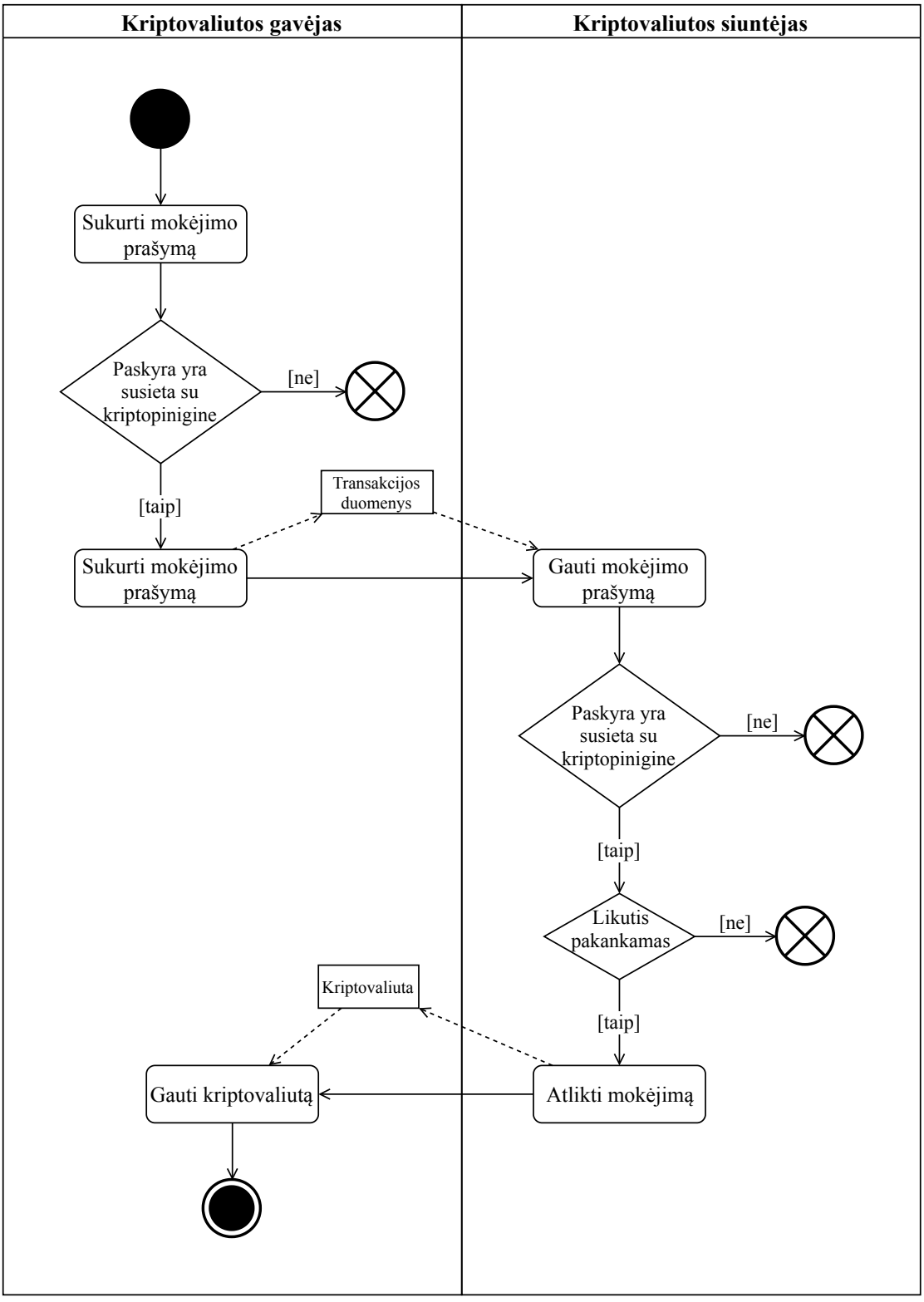
## Maskuotųjų nustatytos tapatybės pranešimų kanalo prenumeravimo veiklų diagrama




27 pav. MAM kanalo prenumeravimo veiklų diagrama

## Priedas nr. 6

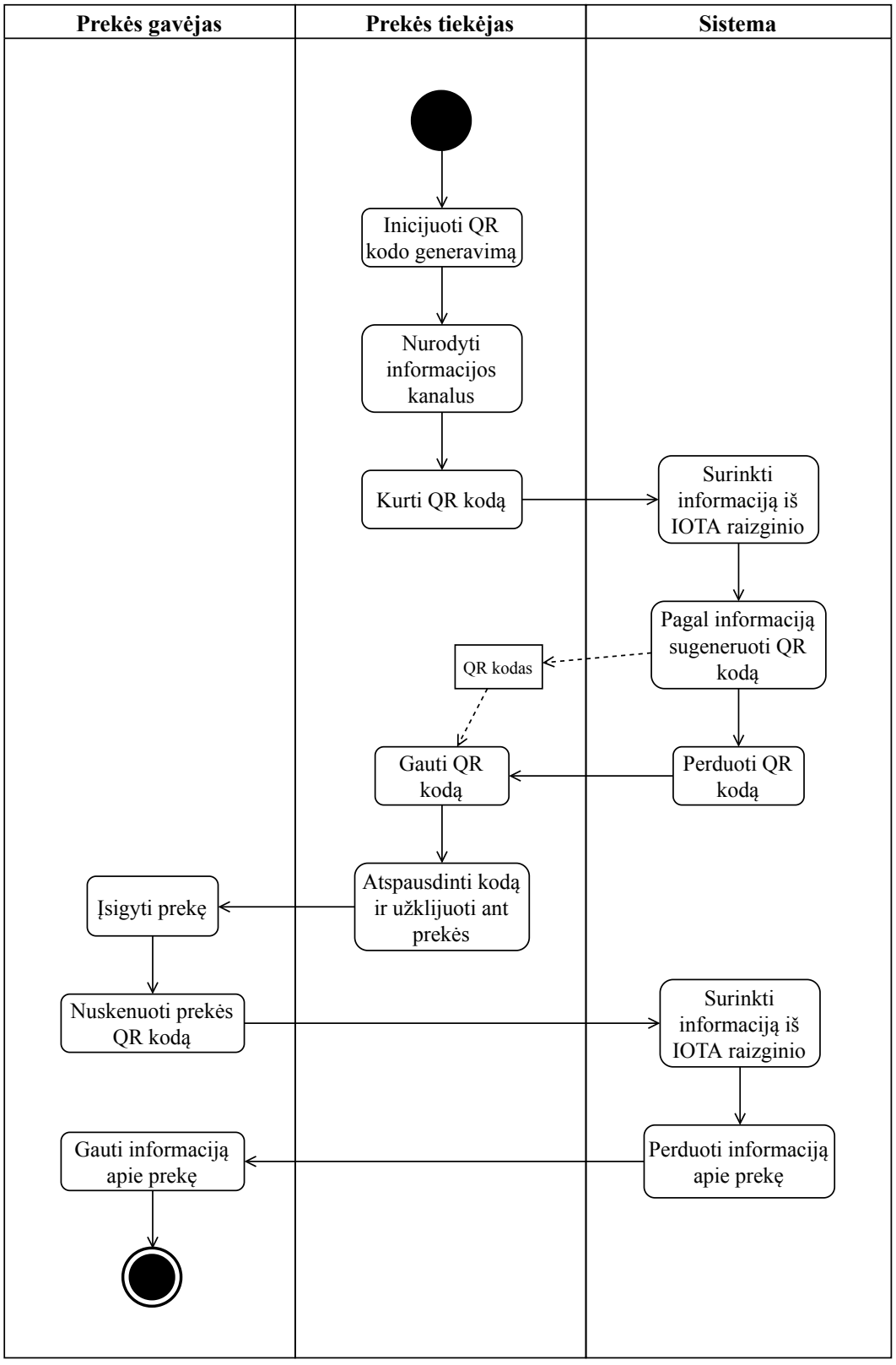
## Kriptovaliutos siuntimo ir gavimo veiklų diagrama




28 pav. Kriptovaliutos siuntimo ir gavimo veiklų diagrama

## Priedas nr. 7

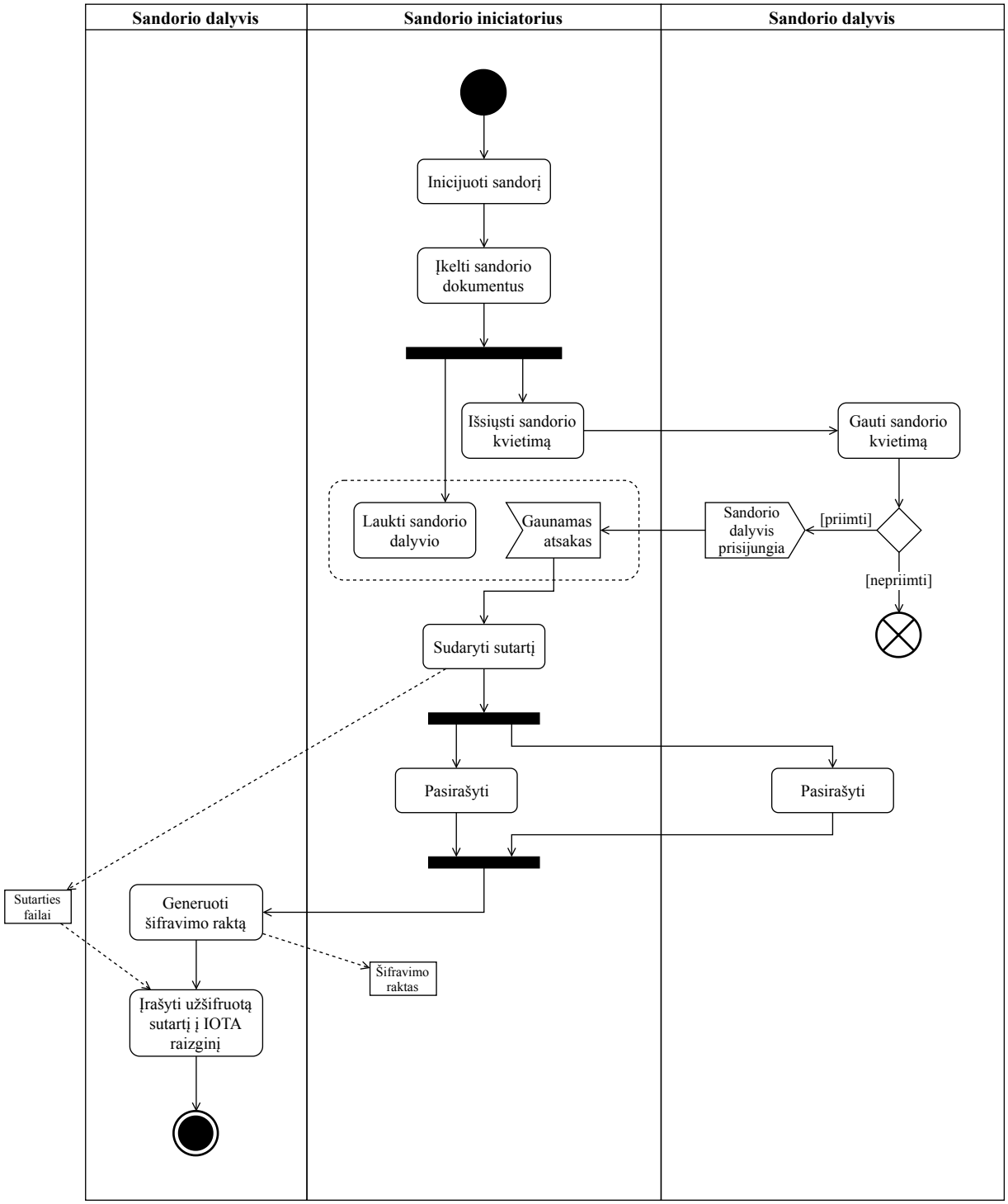
## QR kodo generavimo ir nuskaitymo veiklų diagrama




29 pav. QR kodo generavimo ir nuskaitymo veiklų diagrama

# Priedas nr. 8

# Sandorio sudarymo veiklų diagrama




30 pav. Sandorio sudarymo veiklų diagrama